

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-112950

(43)Date of publication of application : 23.04.1999

(51)Int.Cl.

H04N 7/08
H04N 7/081
H04H 1/00
H04L 9/08
H04L 9/36
// H04N 7/167

(21)Application number : 09-274151

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 07.10.1997

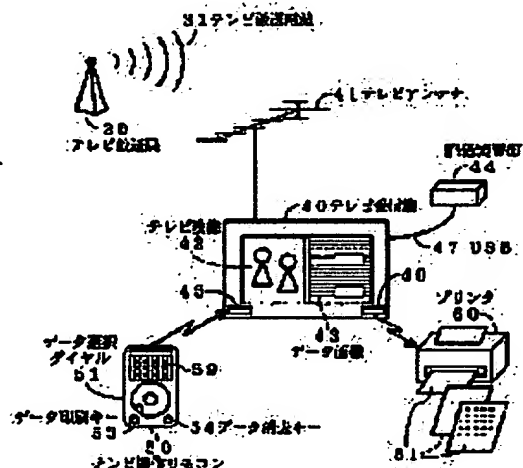
(72)Inventor : ICHIMURA SATORU

(54) ENCRYPTION INFORMATION DECODING REPRODUCING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To distribute in advance encryption information, that is known to only those persons who viewed a television program prior to broadcasting of the television program.

SOLUTION: A broadcast station broadcasts encryption data to be decoded in interlocking with a television program, prior to start of the television program together with program identification information to specify the encryption data. A receiver receives the encryption data and stores the data to an encryption information storage section 6. The broadcast station sends a decoding key to decode the encryption data, in matching with a progress of the program. When a viewer views the program, the receiver receives the decoding key and an encryption information decoding section 9 decodes the encryption data stored in the encryption information storage section 6 by using the decoding key. The decoded encryption data are processed by an encryption information reproduction section 10 and displayed together with a television video image.



LEGAL STATUS

[Date of request for examination]

20.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision]

of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-112950

(43) 公開日 平成11年(1999) 4月23日

(51) Int.Cl.⁸

識別記号

F I

H 0 4 N 7/08
7/081
H 0 4 H 1/00
H 0 4 L 9/08
9/36

H 0 4 N 7/08 Z
H 0 4 H 1/00 F
H 0 4 L 9/00 6 0 1 Z
6 0 1 E
6 8 5

審査請求 未請求 請求項の数14 O L (全 28 頁) 最終頁に続く

(21) 出願番号

特願平9-274151

(22) 出願日

平成9年(1997)10月7日

(71) 出願人 000005496

富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72) 発明者 市村 哲

神奈川県足柄上郡中井町境430 グリーン
テクナカ い 富士ゼロックス株式会社内

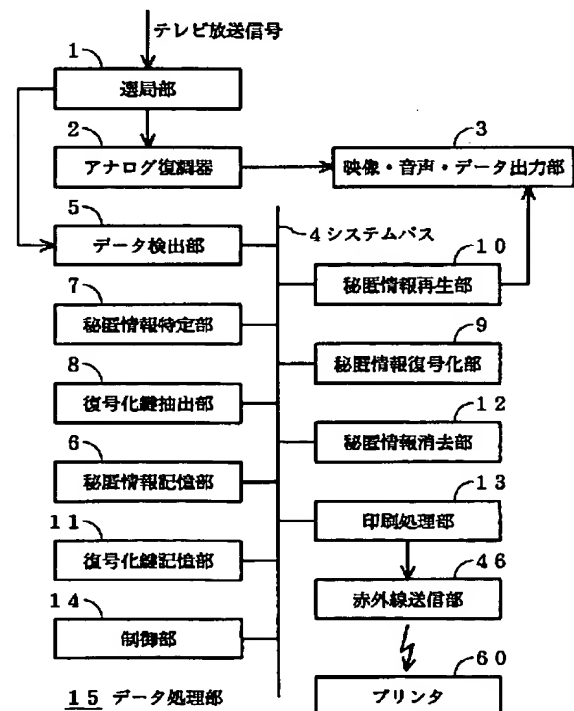
(74) 代理人 弁理士 佐藤 正美

(54) 【発明の名称】 秘匿情報復号再生装置

(57) 【要約】

【課題】 テレビ番組を視聴した人だけが知ることができる秘匿情報をテレビ番組の放送に先立って予め配信することができるようにする。

【解決手段】 放送局は、テレビ番組の開始に先立って、その番組と連動して復号化されるべき、暗号化された秘匿データを、それを特定するための番組識別情報などとともに、放送する。受信機は、その秘匿データを受信して、秘匿情報記憶部6に記憶する。放送局は、番組の進行に合わせて、秘匿データを復号化できる復号化鍵を送信する。視聴者が番組を見ていれば、受信機は、その復号化鍵を受信して、秘匿情報復号化部9で、秘匿情報記憶部6に記憶されている秘匿データを、その復号化鍵によって復号化する。復号化された秘匿データは、秘匿情報再生部10によって処理されて、テレビ映像とともに表示される。



【特許請求の範囲】

【請求項 1】暗号化された情報を秘匿情報として記憶する秘匿情報記憶手段と、

テレビ放送信号またはラジオ放送信号の映像情報または音声情報である映像音声情報を受信する映像音声情報受信手段と、

この映像音声情報受信手段によって受信された映像音声情報を再生する映像音声情報再生手段と、

前記テレビ放送信号またはラジオ放送信号に重畳されたデータを検出するデータ検出手段と、

このデータ検出手段によって検出されたデータに含まれる情報に基づいて、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記映像音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定する秘匿情報特定手段と、

前記データ検出手段によって検出されたデータに含まれる情報から、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵を抽出する復号化鍵抽出手段と、

前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵によって復号化する秘匿情報復号化手段と、

この秘匿情報復号化手段によって復号化された秘匿情報を、前記映像音声情報が再生されるのに伴って再生する秘匿情報再生手段と、

を備えることを特徴とする秘匿情報復号再生装置。

【請求項 2】請求項 1 の秘匿情報復号再生装置において、

前記秘匿情報記憶手段に記憶される秘匿情報は、当該秘匿情報を復号化するための復号化鍵が前記復号化鍵抽出手段によって抽出される時点より前の時点において、前記テレビ放送信号またはラジオ放送信号に重畳されて放送されて、前記データ検出手段によって検出されたものであることを特徴とする秘匿情報復号再生装置。

【請求項 3】請求項 1 の秘匿情報復号再生装置において、

前記秘匿情報記憶手段は、暗号化された情報が秘匿情報として書き込まれた外部記憶装置であることを特徴とする秘匿情報復号再生装置。

【請求項 4】請求項 1～3 のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに復号化鍵記憶手段を備え、

その復号化鍵記憶手段は、前記復号化鍵抽出手段によって抽出された復号化鍵と、この復号化鍵によって復号化可能な前記秘匿情報記憶手段に記憶された秘匿情報を特定する特定情報とを、互いに対応づけて記憶し、

前記秘匿情報復号化手段は、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記復号化鍵記憶手段に記

10

憶された特定情報によって特定された秘匿情報を、前記復号化鍵記憶手段に記憶された復号化鍵によって復号化することを特徴とする秘匿情報復号再生装置。

【請求項 5】請求項 1～4 のいずれかの秘匿情報復号再生装置において、

前記秘匿情報特定手段は、前記データ検出手段によって検出されたデータに含まれる放送番組識別情報によって、前記映像音声情報が再生されるのに伴って復号化されるべき前記秘匿情報記憶手段に記憶された秘匿情報を特定することを特徴とする秘匿情報復号再生装置。

【請求項 6】請求項 1～4 のいずれかの秘匿情報復号再生装置において、

前記秘匿情報特定手段は、前記データ検出手段によって検出されたデータに含まれる放送局識別情報と、この放送局識別情報を含むデータが前記データ検出手段によって検出されたタイミングとに基づいて、前記映像音声情報が再生されるのに伴って復号化されるべき前記秘匿情報記憶手段に記憶された秘匿情報を特定することを特徴とする秘匿情報復号再生装置。

20

【請求項 7】請求項 1～6 のいずれかの秘匿情報復号再生装置において、

前記秘匿情報復号化手段は、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵と、外部メモリ装置に記憶された第 2 の復号化鍵とによって復号化することを特徴とする秘匿情報復号再生装置。

【請求項 8】請求項 7 の秘匿情報復号再生装置において、

30

前記第 2 の復号化鍵は、視聴者または秘匿情報復号再生装置が前記秘匿情報特定手段によって特定された秘匿情報を復号化する権利を有するか否かを識別するために用いられる鍵であって、視聴者または秘匿情報復号再生装置が前記権利を有する場合には、前記復号化鍵抽出手段によって抽出された復号化鍵と、当該第 2 の復号化鍵とによって、前記秘匿情報特定手段によって特定された秘匿情報を正しく復号化できるものであることを特徴とする秘匿情報復号再生装置。

40

【請求項 9】請求項 8 の秘匿情報復号再生装置において、

前記秘匿情報記憶手段に記憶される秘匿情報が、視聴者または秘匿情報復号再生装置ごとに異なる個別暗号化鍵と、全視聴者または全秘匿情報復号再生装置に共通の共通暗号化鍵とによって暗号化されたものであることを特徴とする秘匿情報復号再生装置。

【請求項 10】請求項 1～6 のいずれかの秘匿情報復号再生装置において、

前記復号化鍵抽出手段によって抽出される復号化鍵は、暗号化されたものであり、

50

前記秘匿情報復号化手段は、この復号化鍵抽出手段によ

って抽出された復号化鍵を、外部メモリ装置に記憶された第2の復号化鍵によって復号化し、その復号化された復号化鍵によって、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項 11】請求項 10 の秘匿情報復号再生装置において、

前記第2の復号化鍵は、視聴者または秘匿情報復号再生装置が前記秘匿情報特定手段によって特定された秘匿情報を復号化する権利を有するか否かを識別するために用いられる鍵であって、視聴者または秘匿情報復号再生装置が前記権利を有する場合には、前記復号化鍵抽出手段によって抽出された復号化鍵を、当該第2の復号化鍵によって正しく復号化できるものであることを特徴とする秘匿情報復号再生装置。

【請求項 12】請求項 1～6 のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに暗号化鍵検出手段と暗号化鍵記憶手段とを備え、

前記秘匿情報記憶手段に記憶される秘匿情報は、第1の暗号化鍵によって暗号化されたものであり、

前記暗号化鍵検出手段は、前記第1の暗号化鍵が第2の暗号化鍵と第3の暗号化鍵とによって暗号化されて、前記テレビ放送信号またはラジオ放送信号に重畳されて放送された暗号化鍵情報を検出し、

前記暗号化鍵記憶手段は、この暗号化鍵検出手段によって検出された暗号化鍵情報を、前記秘匿情報記憶手段に記憶された秘匿情報と対応づけて記憶し、

前記復号化鍵抽出手段は、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵として前記第3の暗号化鍵を抽出し、

前記秘匿情報復号化手段は、この復号化鍵抽出手段によって抽出された第3の暗号化鍵と、外部メモリ装置に記憶された、視聴者または秘匿情報復号再生装置ごとに異なる第2の復号化鍵とによって、前記暗号化鍵記憶手段に記憶された暗号化鍵情報を復号化して、前記第1の暗号化鍵を抽出するとともに、この抽出した第1の暗号化鍵を復号化鍵として、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項 13】請求項 1～6 のいずれかの秘匿情報復号再生装置において、

当該秘匿情報復号再生装置は、さらに暗号化鍵検出手段と暗号化鍵記憶手段とを備え、

前記秘匿情報記憶手段に記憶される秘匿情報は、第1の暗号化鍵によって暗号化されたものであり、

前記暗号化鍵検出手段は、前記第1の暗号化鍵が第3の暗号化鍵によって暗号化され、さらにその暗号化された情報が第2の暗号化鍵によって暗号化されて、前記テレ

ビ放送信号またはラジオ放送信号に重畳されて放送された暗号化鍵情報を検出し、

前記暗号化鍵記憶手段は、この暗号化鍵検出手段によって検出された暗号化鍵情報が、外部メモリ装置に記憶された、視聴者または秘匿情報復号再生装置ごとに異なる第2の復号化鍵によって復号化された暗号化鍵情報を、前記秘匿情報記憶手段に記憶された秘匿情報と対応づけて記憶し、

前記復号化鍵抽出手段は、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵として前記第3の暗号化鍵を抽出し、

前記秘匿情報復号化手段は、この復号化鍵抽出手段によって抽出された第3の暗号化鍵によって、前記暗号化鍵記憶手段に記憶された暗号化鍵情報を復号化して、前記第1の暗号化鍵を抽出するとともに、この抽出した第1の暗号化鍵を復号化鍵として、前記秘匿情報特定手段によって特定された秘匿情報を復号化することを特徴とする秘匿情報復号再生装置。

【請求項 14】請求項 12 または 13 の秘匿情報復号再生装置において、

前記第1の暗号化鍵が、全視聴者または全秘匿情報復号再生装置に共通のものであり、前記第2の暗号化鍵が、視聴者または秘匿情報復号再生装置ごとに異なるものであり、前記第3の暗号化鍵が、全視聴者または全秘匿情報復号再生装置に共通のものであることを特徴とする秘匿情報復号再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、テレビ放送またはラジオ放送を受信し、受信したテレビまたはラジオの映像または音声と関連する暗号化された秘匿情報を、テレビまたはラジオの映像または音声の再生タイミングに合わせて復号化して、テレビまたはラジオの映像または音声に伴って再生する装置に関する。なお、この明細書では、「テレビジョン」を「テレビ」と称する。

【0002】

【従来の技術】従来のインターネットは、ユーザが自分の欲しい情報を能動的に取りに行くという利用形態で用いられることが多い。この利用形態は、「PULL型」と呼ばれている。これに対して、ユーザが情報を能動的に取りに行くのではなく、放送局からユーザに対してデータが次々と送られてくる「PUSH型」の利用形態でインターネットが用いられることが増えてきた。PUSH型サービスで送られたデータは、ユーザのパソコン表示画面上に次々と表示される。

【0003】しかしながら、一般家庭でインターネットを利用する場合には、電話回線をインターネットプロバイダに接続するが多い。そのため、放送局から随時送られてくるPUSH型データを受信するには、電話をインターネットプロバイダに常時かけっぱなしにする必

10

20

30

40

50

要があり、電話代が非常に高額になるという問題がある。

【0004】一方、地上波テレビ放送信号の垂直帰線消去期間(VBI)を利用してHTML(Hyper Text Makeup Language)書式のインターネットデータを重畳して放送する「Webキャスト」(出典:インターネットアスキー、Vol. 2, No. 5, pp. 166-167, 1997年5月号)が米国で開始されている。日本では1996年4月から、地上波テレビ放送信号の21ライン分の垂直帰線消去期間中の4ラインがデータ多重放送として割り当てられ、この4ラインの伝走路によってWebキャストが行われている。

【0005】また、衛星デジタルテレビ放送でも、デジタル化した映像情報および音声情報にHTML書式のインターネットデータを重畳して放送する試みが開始されている。デジタルテレビ放送の場合には、映像情報、音声情報およびデータの三者を統一的にデジタル情報として扱えるので、垂直帰線消去期間を利用することなくインターネットデータをテレビ電波で放送することができる。

【0006】そして、地上波テレビ放送や衛星デジタルテレビ放送に重畳されて放送されるインターネットデータを受信する場合には、電話回線を用いる必要がないため、放送局から随時送られてくるPUSH型データを非常に安価に常時受信することができる利点がある。

【0007】さらに、データをテレビ放送に重畳する場合には、テレビ映像とデータを連動させてユーザに配信することができる利点がある。これによって、テレビ番組と関連のあるデータを配信することができ、例えば、教育番組などの映像と同時に教材テキストなどのデータを配信して、テレビ画面やパソコン画面にマルチウィンドウで表示する、といった使い方が可能になる。また、テレビ放送の内容や話題が変わるたびに新たなデータを放送することによって、内容や話題に追従してデータ内容を変えることができるようになる。

【0008】また、日本で放送開始が計画されているBitcast/VBIサービス(出典:日経マルチメディア、pp. 52-59, 1997年4月号)の受信機を利用する場合には、テレビ放送によって送信されたインターネットデータを受信機の記憶装置に一旦蓄積しておき、その蓄積されたインターネットデータを放送番組と連動させて表示することができる。すなわち、テレビ番組やテレビコマーシャルと連動するデータを予めデータ放送によって放送しておき、そのテレビ番組やテレビコマーシャルが始まった瞬間に画面上に表示させることができる。

【0009】

【発明が解決しようとする課題】ところで、Webページ(インターネットデータ)の中には、情報提供者によ

って許可された人以外の人は見るできないようにされているページがある。一般的には、これらの秘匿Webページにはパスワードが設定され、このパスワードを知る人のみが、その秘匿Webページにアクセスできるようになっている。

【0010】このように、ユーザが自分の欲しい情報を能動的に取りに行くという「PULL型」の利用形態でインターネットを利用する場合には、情報提供者は、秘匿したいWebページにパスワードを設定することによって、適切なユーザからのアクセスのみを許すWebページをインターネット上に公開することができる。

【0011】そこで、テレビ映像と連動して表示されるべきWebページについても、情報提供者が許可した視聴者にだけアクセスを許すWebページを放送または公開することができれば、非常に便利である。例えば、秘匿Webページをテレビ番組の開始時刻に先立って放送し、情報提供者が許可した視聴者だけがテレビ番組の進行に合わせて、その秘匿Webページを読み出して見ることができるようにする、というものである。

【0012】しかしながら、前述のBitcast/VBIサービスのよう、PUSH型サービスによってデータを配信する場合には、受信機の記憶装置に蓄積されたデータは、誰もが、いつでも見ることができるため、適切なユーザからのアクセスのみを許すWebページを、テレビ番組の放送時刻に先立って予め配信しておくことはできないという問題がある。

【0013】公知の暗号技術を利用して、この問題を解決する方法として、放送局は、テレビ番組に関連したデータを暗号化して放送し、受信機では、その暗号化データを受信して記憶装置に記憶し、視聴者は、その記憶された暗号化データを別途、電子メールや郵便はがきによって放送局から送られた復号化鍵(パスワードなど)を用いて復号化する、という方法が考えられる。

【0014】例えば、放送局から送られる電子メールや郵便はがきに、復号化鍵のほかに、その復号化鍵を利用できる放送番組名が書かれていれば、復号化鍵を入手した視聴者は、放送局によって指定された放送番組に関連する暗号化データのみを復号化することができる。

【0015】しかしながら、この方法の場合、テレビ番組と連動して再生されるべき秘匿データを再生するためには、視聴者は、受信機の記憶装置に記憶された暗号化データの中から、当該テレビ番組に関連する暗号化データを検索し、その検索した暗号化データを、電子メールや郵送によって放送局から送られた復号化鍵によって復号化する必要があり、この操作のために、視聴しているテレビ番組に集中できないという問題がある。

【0016】しかも、同一のテレビ番組内であっても、番組の進行または秘匿データの内容に応じて、秘匿データを視聴できる人を動的に変えたい場合もあり、このような場合には、放送局から予め電子メールや郵送によ

10

20

30

40

50

て復号化鍵を送付しておくことは極めて困難であるという問題もある。

【0017】さらに、電子メールや郵送によって放送局から送られた復号化鍵によって暗号化データを復号化する場合には、視聴者は復号化鍵を入手した時点以降のタイミングであれば、いつでも暗号化データを復号化できてしまうために、テレビ番組と連動して再生されるべき秘匿データをテレビ番組の放送開始以前のタイミングでは視聴できないようにするなどの、時間制限を付けたアクセス制御をすることができないという問題がある。

【0018】また、特開平9-139933号公報には、秘匿データを保持するデータベースにアクセスするための方法として、放送局が、データベースアクセスのための案内情報をテレビ映像に重畳して放送し、視聴者は、その受信したデータベースアクセスのための案内情報と、視聴者自身が知るパスワードとを入力して、電話回線を通じてデータベースにアクセスすることにより、秘匿データを入手する方法が示されている。

【0019】しかしながら、この方法は、電話回線を使用する必要があるので、通信コストがかかるという問題がある。また、電話回線に接続するための通信装置を備える必要があるため、テレビ受信システムが複雑になるという問題がある。さらに、この場合に視聴者が入力すべきパスワードは別途、電子メールや郵送によって入手する必要があり、前述したように手間がかかるという問題がある。

【0020】ところで、テレビコマーシャルを視聴者に見てもらう方法の一つとして、スポンサーが提供するテレビ番組を見た視聴者だけに、そのスポンサーからのプレゼントを送る場合があるが、同様にテレビ番組を見た視聴者だけに、有益な情報や特別の権利を提供することによって、スポンサーが放送したテレビコマーシャルをより多くの視聴者に見てもらうことができる。

【0021】例えば、テレビ番組と連動して動作するコンピュータプログラムを予め放送しておき、テレビ番組を見た視聴者だけに、そのコンピュータプログラムを実行する権利を与えるようにすることができれば、コンピュータプログラムを実行したい視聴者がテレビ番組を見るようになるので、テレビコマーシャルを視聴者に見てもらう方法として、非常に有益である。

【0022】しかしながら、前述したように、PUSH型サービスによってデータを配信する場合には、受信機の記憶装置に蓄積されたデータは、誰もが、いつでも見ることができるため、テレビ番組を見た視聴者だけにアクセスを許すWebページを、テレビ番組の放送時刻に先立って予め配信しておくことはできないという問題がある。

【0023】日本国内で放送が開始されている衛星デジタルテレビ放送「PerfectTV!」では、スクランブル映像と、このスクランブル映像を復号化するための

復号化鍵とを同時に放送するようになっているが、この場合にも、テレビ番組で使用するデータやプログラムを、テレビ番組の放送時刻に先立って予め視聴者に配信しておくことはできない。

【0024】すなわち、PerfectTV!の場合には、テレビ番組と連動して復号化されるべき秘匿データが大量に存在する場合でも、秘匿データを利用するタイミングで秘匿データを放送する必要がある。さらに、同一の秘匿データを複数の場面または番組で利用する場合でも、放送局は秘匿データを利用するタイミングで毎回、当該秘匿データを放送しなければならないという問題がある。

【0025】さらに、PerfectTV!の場合には、スクランブル映像と、このスクランブル映像を復号化するための復号化鍵とを同時に配信するようになっているため、CDROMなどの放送以外のメディアによって視聴者に提供された秘匿データを、テレビ番組と連動させて復号化し、再生するというようなことができないという問題がある。

【0026】以上の点から、この発明は、(1)テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、(2)テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができ、(3)テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができ、(4)視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、

(5)同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができ、(6)CDROMなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる、ようにすることにある。

【0027】

【課題を解決するための手段】この発明では、秘匿情報復号再生装置として、暗号化された情報を秘匿情報として記憶する秘匿情報記憶手段と、テレビ放送信号またはラジオ放送信号の映像情報または音声情報である映像音声情報を受信する映像音声情報受信手段と、この映像音声情報受信手段によって受信された映像音声情報を再生する映像音声情報再生手段と、前記テレビ放送信号またはラジオ放送信号に重畳されたデータを検出するデータ検出手段と、このデータ検出手段によって検出されたデータに含まれる情報に基づいて、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記映像音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定する秘匿情報特定手段と、前記データ検出手段によって検

出されたデータに含まれる情報から、前記秘匿情報特定手段によって特定された秘匿情報を復号化するための復号化鍵を抽出する復号化鍵抽出手段と、前記秘匿情報記憶手段に記憶された秘匿情報のうちの、前記秘匿情報特定手段によって特定された秘匿情報を、前記復号化鍵抽出手段によって抽出された復号化鍵によって復号化する秘匿情報復号化手段と、この秘匿情報復号化手段によって復号化された秘匿情報を、前記映像音声情報が再生されるのに伴って再生する秘匿情報再生手段と、を設ける。

【0028】この場合、前記秘匿情報記憶手段に記憶される秘匿情報は、当該秘匿情報を復号化するための復号化鍵が前記復号化鍵抽出手段によって抽出される時点より前の時点において、前記テレビ放送信号またはラジオ放送信号に重畳されて放送されて、前記データ検出手段によって検出されたものとして行うことができる。

【0029】あるいはまた、前記秘匿情報記憶手段は、暗号化された情報が秘匿情報として書き込まれた外部記憶装置とすることができる。

【0030】なお、この明細書では、暗号化された情報だけでなく、その暗号化された情報を復号化した情報も、便宜上、秘匿情報と称する。

【0031】

【作用】上記のように構成した、この発明の秘匿情報復号再生装置においては、放送局がテレビまたはラジオの番組の放送に先立って予め、その番組と連動して復号化されるべき秘匿情報を放送することによって、番組放送前に、その番組と連動して復号化されるべき秘匿情報が、秘匿情報記憶手段に記憶されるようになる。あるいはまた、放送局が番組の放送に先立って予め、その番組と連動して復号化されるべき秘匿情報が書き込まれた、CDROMなどの外部記憶装置を視聴者に配布することによって、秘匿情報記憶手段は、番組放送前に、その番組と連動して復号化されるべき秘匿情報を記憶した状態となる。

【0032】このように秘匿情報記憶手段に秘匿情報が記憶された状態で、番組開始とともに放送局が、当該番組の映像情報または音声情報が再生されるのに伴って復号化されるべき秘匿情報を特定することができる、放送番組識別情報などの情報と、これによって特定される秘匿情報を復号化するための復号化鍵とを放送することによって、秘匿情報復号再生装置においては、秘匿情報特定手段によって、秘匿情報記憶手段に記憶された秘匿情報のうちの、当該番組の映像情報または音声情報が再生されるのに伴って復号化されるべき秘匿情報が特定され、復号化鍵抽出手段によって、その特定された秘匿情報を復号化するための復号化鍵が抽出され、秘匿情報復号化手段によって、その特定された秘匿情報が、その抽出された復号化鍵によって復号化され、秘匿情報再生手段によって、その復号化された秘匿情報が、当該番組の

映像情報または音声情報が再生されるのに伴って、画像または音声として再生される。

【0033】したがって、テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができるとともに、CDROMなどの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる。

【0034】さらに、放送局で復号化鍵の送信や内容を調整することによって、テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができるとともに、テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができるようになる。

【0035】

【発明の実施の形態】この発明の実施形態を、この発明をテレビ放送の送受信システムに適用した場合につき示す。ただし、後述するように、この発明はラジオ放送の送受信システムにも適用することができる。

【0036】なお、「特許請求の範囲」および「課題を解決するための手段」では、「映像情報または音声情報」を「映像音声情報」と定義したが、以下の実施形態は、この発明をテレビ放送の送受信システムに適用した場合であるので、以下の実施形態では、「映像音声情報」は「映像情報および音声情報」を意味するものとする。

【0037】〔第1の実施形態〕第1の実施形態では、放送局は、テレビ番組の開始に先立って予め、テレビ放送によって秘匿データを放送し、テレビ番組の進行に合わせて、先に放送した秘匿データを復号化するための復号化鍵を放送する。テレビ受信機を含む受信システムでは、先に放送された秘匿データを秘匿情報記憶部に記憶し、テレビ番組の進行に合わせて放送された復号化鍵を検出して、この復号化鍵によって秘匿情報記憶部に記憶された秘匿データを復号化して、画像または音声として表示または再生する。

【0038】ただし、以下においては、秘匿データが画像として表示されるものである場合についてのみ示す。

【0039】また、第1の実施形態は、この発明を地上波テレビ放送の送受信システムに適用した場合である。

【0040】（構成）図1は、第1の実施形態の送受信システムの一例を示す。テレビ放送局30は、テレビ放送電波31によって、地上波テレビ放送として、変調されたアナログ映像音声信号を送信するとともに、例え

ば、テレビ映像信号の垂直帰線消去期間中の第10ラインから第13ラインまでの4ラインを利用して、秘匿データや復号化鍵などのデジタルデータを送信する。1ライン当たり9.6kbpsの伝送容量があるので、4ライン分では38.4kbpsのデータを伝送することができる。

【0041】この例の場合、送信されるデジタルデータは、HTML書式のインターネットデータであり、秘匿データについては暗号化されたものである。典型的なインターネットデータは、レイアウト情報、プレーンテキスト、動画、静止画、音声、他のインターネットデータへのリンク情報、またはコンピュータプログラムを含む。

【0042】受信システムは、全体として、テレビ受信機40、テレビアンテナ41、記憶装置部44、テレビ操作リモコン50、およびプリンタ60を備え、テレビ放送局30からの、変調されたアナログ映像音声信号、および秘匿データや復号化鍵などのデジタルデータを含むテレビ放送信号は、テレビアンテナ41で受信されて、テレビ受信機40内の選局部で選局される。

【0043】テレビ受信機40は、その表示画面上にテレビ映像42とインターネットデータによるデータ画像43とを同時に表示できるようにし、通常は、表示画面全体にテレビ映像42を表示するが、秘匿データを受信して秘匿情報記憶部に記憶し、その後、この秘匿データを復号化するための復号化鍵を受信して、その復号化鍵によって秘匿情報記憶部に記憶されている秘匿データを復号化したときには、その復号化したインターネットデータによるデータ画像43を、テレビ映像42と同時に表示するようにする。

【0044】テレビ映像42とデータ画像43とを同時に表示する方法としては、図示するように表示画面を横方向に2分割する方法以外に、いわゆるピクチャインピクチャ方式や、表示画面全体にテレビ映像42を表示し、それにオーバーラップさせる形で、テレビ映像42上の複数の領域に分散させてデータ画像43を表示する方法などを用いることができる。さらに、テレビ受信機40の表示部とは別の表示装置にデータ画像43を表示するようにしてもよい。

【0045】記憶装置部44は、上記の秘匿情報記憶部および後述する復号化鍵記憶部を構成するもので、記憶媒体として、ハードディスク（磁気ディスク）、光磁気ディスク、フラッシュメモリなどを用い、USB（Universal Serial Bus）47によってテレビ受信機40と接続する。これによって、テレビ受信機40と記憶装置部44との間では12Mbpsでデータを転送することができる。

【0046】ただし、記憶装置部44はテレビ受信機40内に設置してもよい。また、記憶装置部44の記憶媒体として、MD、ZIPディスク、PCMPICIA対応

フラッシュメモリカードなどの交換可能な記録媒体を利用すれば、容易に記憶容量を増やすことができるようになる。

【0047】テレビ操作リモコン50は、テレビ受信機40の赤外線受信部45に赤外線リモコン信号を送信して、テレビ受信機40を制御するもので、データ選択ダイヤル51、データ印刷キー53、データ消去キー54、およびその他のキー群59を有する。その他のキー群59は、通常のテレビ操作リモコンが備える電源スイッチ、選局キー、音量調節キーなどである。

【0048】データ選択ダイヤル51は、これを回すことによって、記憶装置部44の秘匿情報記憶部に記憶されている秘匿データから、再表示すべき秘匿データを選択するものである。後述するように、その選択された秘匿データは、記憶装置部44の復号化鍵記憶部に記憶されている、その選択された秘匿データを復号化するための復号化鍵によって復号化されて、データ画像43として再表示される。

【0049】データ印刷キー53は、秘匿データが復号化鍵によって復号化されて表示されているときに、またはデータ選択ダイヤル51によって再表示すべき秘匿データを選択して再表示した状態で、これを押下することによって、その表示または再生された秘匿データをプリンタ60によって用紙61上に画像として印刷するものである。

【0050】この場合、復号化された秘匿データは、テレビ受信機40の赤外線送信部46で赤外線信号とされてプリンタ60に送信される。この赤外線伝送は、IrDA1.1規格に準拠したもので、4Mbpsで印刷データを転送することができる。

【0051】データ消去キー54は、これを押下することによって、後述するように、記憶装置部44の秘匿情報記憶部に記憶されている秘匿データを消去するものである。

【0052】図2は、第1の実施形態の秘匿情報復号再生装置の機能ブロック構成を示す。この実施形態の秘匿情報復号再生装置は、選局部1、アナログ復調部2、映像・音声・データ出力部3、およびデータ処理部15を備える。

【0053】変調されたアナログ映像音声信号、および秘匿データや復号化鍵などのデジタルデータを含むテレビ放送信号は、選局部1で選局され、その選局されたテレビ放送信号中の変調されたアナログ映像音声信号が、アナログ復調部2で復調され、その復調されたアナログ映像音声信号が、映像・音声・データ出力部3に供給される。映像・音声・データ出力部3は、図1に示したテレビ受信機40の表示部およびスピーカによって構成され、表示部の表示画面にテレビ映像およびデータ画像が表示され、スピーカからテレビ音声再生される。

【0054】データ処理部15は、システムバス4に対

して、データ検出部 5、秘匿情報記憶部 6、秘匿情報特定部 7、復号化鍵抽出部 8、秘匿情報復号化部 9、秘匿情報再生部 10、復号化鍵記憶部 11、秘匿情報消去部 12、印刷処理部 13、および制御部 14 が、それぞれ接続されて構成される。

【0055】ただし、データ処理部 15 は、実装的には、1つのブロックが幾つかの機能部分を含むように、または 1つの機能部分が幾つかのブロックに分割されるように、構成することができる。

【0056】データ検出部 5 は、選局部 1 で選局されたテレビ放送信号中の、秘匿データや復号化鍵などのデジタルデータを検出して、システムバス 4 に出力する。

【0057】秘匿情報記憶部 6 は、データ検出部 5 によって検出されたデータに含まれる秘匿データを記憶するもので、上述したように記憶装置部 44 に設けられる。

【0058】秘匿情報特定部 7 は、データ検出部 5 によって検出されたデータに含まれる後述する放送番組識別情報などの情報に基づいて、秘匿情報記憶部 6 に記憶された秘匿データのうちの、テレビの映像および音声が生再生されるのに伴って復号化されるべき秘匿データを特定する。

【0059】復号化鍵抽出部 8 は、データ検出部 5 によって検出されたデータに含まれる情報から、秘匿情報特定部 7 によって特定された秘匿データを復号化するための復号化鍵を抽出する。

【0060】秘匿情報復号化部 9 は、秘匿情報記憶部 6 に記憶された秘匿データのうちの、秘匿情報特定部 7 によって特定された秘匿データを、復号化鍵抽出部 8 によって抽出された復号化鍵によって復号化する。

【0061】秘匿情報再生部 10 は、秘匿情報復号化部 9 によって復号化された秘匿データ、すなわち、この例では HTML 書式のインターネットデータを、表示するように処理して、映像・音声・データ出力部 3 に出力する。

【0062】復号化鍵記憶部 11 は、復号化鍵抽出部 8 によって抽出された復号化鍵を記憶するもので、上述したように記憶装置部 44 に設けられる。

【0063】秘匿情報消去部 12 は、テレビ操作リモコン 50 のデータ消去キー 54 が押下されることによって、後述するように秘匿情報記憶部 6 から秘匿データを消去する。

【0064】印刷処理部 13 は、テレビ操作リモコン 50 のデータ印刷キー 53 が押下されることによって、後述するように秘匿データをプリンタ 60 で印刷させるように処理して、赤外線送信部 46 に出力する。

【0065】制御部 14 は、秘匿情報復号再生装置全体の処理を制御するものである。なお、必要に応じて、データ伝送エラーを訂正するエラー訂正部をシステムバス 4 に接続する。

【0066】(秘匿データ受信記憶時の動作) 第 1 の実

施形態では、まず、テレビ放送局 30 は、テレビ番組の開始時刻より前の時点において、そのテレビ番組と連動すべきデータを、秘匿データとして暗号化して、テレビ映像信号の垂直帰線消去期間を利用して放送する。

【0067】この場合の暗号化方式としては、例えば、IDEA (International Data Encryption Algorithm) を用いる。IDEA は、スイス連邦工科大学において開発された暗号化方式であり、情報を暗号化するための暗号化鍵と、この暗号を解くための復号化鍵とが同一の鍵である共有鍵暗号方式 (または秘密鍵暗号方式) である。鍵のビット長は 128 と定められている。IDEA 暗号方式は、暗号メールソフト PGP (Pretty Good Privacy) にも使われており、鍵が 128 ビット長の IDEA は、現在主流の DES (鍵は 56 ビット長)、トリプル DES (鍵は 112 ビット長) よりも、安全性が高いと言われている。

【0068】なお、データを暗号化する暗号化方式としては、共有鍵暗号方式以外にも、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせたハイブリッド暗号方式を用いることができる。公開鍵暗号方式とは、暗号化鍵 (公開鍵) と復号化鍵 (秘密鍵) とが異なる場合の暗号化方式であり、RSA が代表的な方式である。公開鍵暗号方式を用いる場合には、テレビ放送局 30 は、公開鍵で暗号化したデータを放送する。また、ハイブリッド暗号方式は、暗号化すべきデータごとにランダムなセッション鍵を作成して、そのセッション鍵でデータを暗号化し、次に、公開鍵暗号方式の公開鍵でセッション鍵を暗号化して、暗号化されたデータと暗号化されたセッション鍵とを一緒にして放送する方式である。

【0069】さらに、この実施形態では、テレビ放送局 30 は、放送する秘匿データに対して、当該秘匿データを参照するテレビ番組の放送番組識別情報を付加して放送する。この放送番組識別情報としては、例えば、Gコード (VCR・PLUS と呼ばれる、米国ジェムスター社製のテレビ番組識別コード) を用いる。

【0070】そして、第 1 の実施形態の秘匿情報復号再生装置では、以下のように、テレビ放送局 30 によって放送された秘匿データが受信され、秘匿情報記憶部 6 に記憶される。

【0071】すなわち、図 3 は、この場合のデータ処理部 15 が行う受信記憶処理ルーチンを示し、その受信記憶処理ルーチン 100 では、まずステップ 101 において、データ検出部 5 でデジタルデータを検出したか否かを判断する。

【0072】この例では、そのデジタルデータは、MIME (Multipurpose Internet Mail Extensions) 構文で表現されたものである。図 4 は、その MIME 構文で表現されたデジ

ルデータの一例を示し、1つのデジタルデータ中に複数のオブジェクトを格納するために、マルチパートタイプを利用しており、図4の例では、"-----
-----2424F803488"によって、各オブジェクトが区切られている。

【0073】このうちの1つめのオブジェクトは、"Content-Type:text/control"以下に記述された内容である。"Content-Type:text/control"以下の部分には、テレビ受信機40が当該デジタルデータをどのように処理すべきかを記述するようになっており、図4の例では、当該デジタルデータを表示（または再生）すべきタイミングを記述している。

【0074】"<program gcode=425334 id=32>"の部分が、その表示タイミングを記述した部分であり、当該デジタルデータを表示すべきテレビ番組の番組識別子と、このテレビ番組中でのデジタルデータのデータ識別子とが記述されている。すなわち、テレビ受信機40が、Gコード番号が425334のテレビ番組を受信している最中に、デジタルデータ識別子が32のデジタルデータの表示開始命令を受信した場合には、そのタイミングで当該デジタルデータをテレビ受信機40に表示することとなる。

【0075】なお、デジタルデータを表示すべきタイミングを示す情報は、絶対時刻、または番組開始時点からの相対時間でもよい。

【0076】一方、2つめのオブジェクトは、"Content-Type:application/encrypted-by-idea"以下に記述された内容である。"Content-Type:application/encrypted-by-idea"以下の部分には、IDEA暗号方式で暗号化された秘匿データを記述するようになっている。ここで、"application/encrypted-by-idea"という構文は、IDEA暗号を処理するアプリケーションを実行して、当該オブジェクトを処理すべきことを示す構文である。

【0077】また、図4の例のように、"Content-Transfer-Encoding:base64"の記述がある場合には、暗号化された秘匿データをさらにbase64形式にエンコードして記述するようになっている。Base64は、バイナリデータの8ビット×3バイトを6ビット×4バイトに振り分けて、それを通信データの7ビットに変換する方法である。

【0078】なお、複数の情報を多重化する方法としては、MIMEエンコードを用いる代わりに、MPEG-2 Systemsに準拠したパケット多重方式を用いてもよい。MPEG-2 Systemsでは、TS (Transport Stream) パケットと呼ぶ188バイト固定長のパケットを伝送の基本単位としており、

このTSパケットのパケットヘッダにパケット識別のためのPID (Packet Identifier) を含む構造となっている。

【0079】データ検出部5が、デジタルデータとして上記のMIMEデータを検出したときには、ステップ102に進んで、データ検出部5は、その検出したMIMEデータをデコードする。

【0080】受信記憶処理ルーチン100では、次にステップ103において、そのデコードされたデータ、すなわち、MIMEデータから抽出された秘匿データ、その秘匿データについての暗号化方式、およびその秘匿データを特定するための識別情報を、秘匿情報記憶部6に記憶する。

【0081】図5は、秘匿情報記憶部6における記憶状態の一例を示す。同図に示すように、秘匿情報記憶部6は、秘匿データと、その秘匿データについての暗号化方式と、その秘匿データを特定するための識別情報であるGコード（テレビ番組識別子）およびID（デジタルデータ識別子）とを、対応づけて記憶する。

【0082】（秘匿データ復号再生時の動作）上述したように秘匿データを放送した後、テレビ放送局30は、テレビ番組の進行に合わせて、秘匿データを復号化するための復号化鍵を放送する。第1の実施形態では、上述したように、復号化鍵もテレビ映像信号の垂直帰線消去期間を利用して放送する。

【0083】そして、第1の実施形態の秘匿情報復号再生装置では、以下のように、テレビ放送局30によって放送された復号化鍵が受信され、その復号化鍵によって秘匿情報記憶部6に記憶されている秘匿データが復号化されて、画像として表示される。

【0084】すなわち、図6は、この場合のデータ処理部15が行う復号再生処理ルーチンを示し、その復号再生処理ルーチン200では、まずステップ201において、データ検出部5でデジタルデータを検出したか否かを判断する。

【0085】この例では、そのデジタルデータも、MIME構文で表現されたものである。図7は、そのMIME構文で表現されたデジタルデータの一例を示し、図4において上述したように、"Content-Type:text/control"以下の部分は、テレビ受信機40が当該デジタルデータをどのように処理すべきかを記述している部分であり、図7の例では、添付した復号化鍵によって、秘匿情報記憶部6に記憶されている秘匿データを復号化し、再生するように指示している。

【0086】"<play gcode=425334 id=32 decryption-key-base64=GTvb7ujJn85bBG4VfyF7G1==>"という構文は、Gコード番号が425334であり、かつデジタルデータ識別子が32である秘匿デ

10

20

30

40

50

ータが、秘匿情報記憶部6に記憶されているならば、復号化鍵”G T v b 7 u j J n 8 5 b B G 4 V f y F 7 G 1 ==” (128bit)を用いて、その秘匿データを復号化し、正常に復号化できた場合には、テレビ受信機40に表示するように指示する命令文である。この例では、復号化鍵はbase64によってエンコードされている。

【0087】データ検出部5が、デジタルデータとして上記のMIMEデータを検出したときには、ステップ202に進んで、データ検出部5は、その検出したMIMEデータをデコードし、復号化鍵抽出部8は、そのデコードされたデータから復号化鍵を抽出する。

【0088】次に、ステップ203において、秘匿情報特定部7は、そのデコードされたデータ、すなわちMIMEデータから抽出された情報中の、秘匿データ特定情報、図7の例では”gcode=425334 id=32”という情報に基づいて、秘匿情報記憶部6に記憶されている秘匿データを検索して、テレビ番組と連動して復号化すべき秘匿データを特定できるか否かを判断する。

【0089】例えば、テレビ番組の開始前の秘匿データの放送時に、視聴者がテレビ放送を受信していなかった場合には、秘匿情報記憶部6には、秘匿データ特定識別情報によって特定されるべき秘匿データが記憶されていないので、ステップ203では特定不能と判断されて、ステップ201に戻る。

【0090】ステップ203で、秘匿情報特定部7が、テレビ番組と連動して復号化すべき秘匿データを特定できると判断したときには、ステップ204に進んで、秘匿情報特定部7は、テレビ番組と連動して復号化すべき秘匿データを特定する。

【0091】さらに、ステップ205において、秘匿情報復号化部9は、その秘匿情報特定部7によって特定された、秘匿情報記憶部6に記憶されている秘匿データを、ステップ202で復号化鍵抽出部8によって抽出された復号化鍵、図7の例では復号化鍵”G T v b 7 u j J n 8 5 b B G 4 V f y F 7 G 1 ==”を用いて復号化する。この復号化の際には、秘匿情報記憶部6に記憶されている暗号化方式を用いる。

【0092】復号再生処理ルーチン200では、さらにステップ206において、復号化鍵抽出部8によって抽出された復号化鍵を、復号化鍵記憶部11に記憶する。この場合、図8に一例を示すように、復号化鍵記憶部11には、復号化鍵と、その復号化鍵の復号化鍵記憶部11への記憶時刻と、その復号化鍵によって復号化された秘匿データの秘匿情報記憶部6における記憶位置(図5のNoカラムの値)とを、対応づけて記憶する。

【0093】そして、ステップ207において、ステップ205で秘匿情報復号化部9によって復号化されたデータを、秘匿情報再生部10で処理して、映像・音声・

データ出力部3に出力する。これによって、テレビ番組と連動して表示されるべき秘匿データが、図1に示したように、データ画像43として、テレビ映像42とともに表示される。

【0094】復号再生処理ルーチン200では示していないが、このようにテレビ受信機40にデータ画像43が表示されているタイミングで、視聴者がテレビ操作リモコン50のデータ印刷キー53を押下すると、そのとき表示されている秘匿データが、印刷処理部13で印刷処理されて、赤外線送信部46からプリンタ60に送信され、プリンタ60で画像として印刷される。

【0095】(秘匿データの再表示と消去)第1の実施形態では、復号化鍵記憶部11が設けられて、これに復号化鍵が記憶されるので、復号化鍵記憶部11に復号化鍵が記憶された後においては、視聴者は、復号化鍵記憶部11に記憶されている復号化鍵によって、いつでも、秘匿情報記憶部6に記憶されている秘匿データを復号化して、再表示することができる。

【0096】秘匿データを再表示する場合には、視聴者は、テレビ操作リモコン50のデータ選択ダイヤル51を回して、秘匿情報記憶部6に記録されている秘匿データ、および復号化鍵記憶部11に記憶されている復号化鍵を、次々と呼び出す。

【0097】図8に示して上述したように、復号化鍵記憶部11には、復号化鍵の復号化鍵記憶部11への記憶時刻と、その復号化鍵によって復号化された秘匿データの秘匿情報記憶部6における記憶位置とが記憶されている。

【0098】視聴者がデータ選択ダイヤル51を左に回すと、データ処理部15は、この復号化鍵記憶部11に記憶されている記憶時刻から、復号化鍵記憶部11に最も後に記憶された復号化鍵から順に復号化鍵を特定して、復号化鍵記憶部11から呼び出すとともに、復号化鍵記憶部11に記憶されている秘匿データ記憶位置から、その呼び出される復号化鍵によって復号化される秘匿データを、秘匿情報記憶部6から呼び出す。

【0099】呼び出された秘匿データは、復号化鍵復号化部9において、呼び出された復号化鍵によって復号化され、その暗号化された秘匿データが、秘匿情報再生部10で処理されて、映像・音声・データ出力部3に出力され、テレビ受信機40に再表示される。

【0100】逆にデータ選択ダイヤル51を右に回すと、その時点で再表示されている秘匿データを復号化する復号化鍵より、より後に復号化鍵記憶部11に記録された復号化鍵によって復号化される秘匿データが順次、復号化されて、テレビ受信機40に再表示される。

【0101】このようにデータ選択ダイヤル51の操作によって秘匿データを再表示した状態で、視聴者がテレビ操作リモコン50のデータ印刷キー53を押下すると、そのとき再表示されている秘匿データが、印刷処理

10

20

30

40

50

部 13 で印刷処理されて、赤外線送信部 46 からプリンタ 60 に送信され、プリンタ 60 で画像として印刷される。

【0102】上記の例のように、秘匿情報記憶部 6 に記憶される秘匿データが HTML 書式のインターネットデータである場合には、データ中にリンク情報が埋め込まれている場合があるので、データ選択ダイヤル 51 によってリンクアンカーを指定できるようにしてもよい。

【0103】この場合、指定されたリンクアンカーから辿ったリンク先のデータが、秘匿情報記憶部 6 に記憶された秘匿データであった場合には、この秘匿データの秘匿情報記憶部 6 における記憶位置（図 5 の No カラムの値）を検索キーとして、図 8 に示した復号化鍵記憶部 11 における秘匿データアドレスカラムを検索して、対応する復号化鍵を特定する。そして、この秘匿データを復号化して、テレビ受信機 40 に再表示するようにする。

【0104】秘匿情報記憶部 6 に記憶された秘匿データ中には、テレビ番組放送時に参照される（復号化される）情報もあれば、参照されない（復号化されない）情報もある。しかし、いずれの情報であっても、テレビ番組終了時には消去するようにしても構わない。

【0105】秘匿情報記憶部 6 に記憶されている秘匿データをテレビ番組終了時に消去するには、例えば、視聴者が適当な時点でテレビ操作リモコン 50 のデータ消去キー 54 を押下することによって、秘匿情報消去部 12 が、図 5 に示したように秘匿情報記憶部 6 に記憶されている Gコードに含まれる放送時刻情報から、番組終了時刻を検出して、番組終了時刻を過ぎた秘匿データのみを、秘匿情報記憶部 6 から消去するようにする。または、放送局が、番組終了時に番組終了を通知する信号を放送し、テレビ受信機 40 では、この信号を検知して、秘匿情報消去部 12 が、番組終了時刻を過ぎた秘匿データのみを、秘匿情報記憶部 6 から消去するようにしてもよい。

【0106】（変形例）秘匿データは、複数の特定の復号化鍵を組み合わせた場合にのみ正しく復号化できるものとすることもできる。この場合には、その秘匿データが秘匿情報記憶部 6 に記憶されている状態で、放送局からテレビ番組と連動して順次、送信された複数の復号化鍵を順次、復号化鍵記憶部 11 に記憶し、秘匿データを復号化するための復号化鍵が揃った時点で、秘匿データを復号化するようにする。このようにすることによって、例えば、10 回に渡って連続するドラマの 10 回すべてを視聴した視聴者にだけ、放送局から有益な情報を提供するというようなことができる。

【0107】地上波テレビ放送の放送電波によって秘匿データまたは復号化鍵を伝送する方法としては、テレビ映像信号の垂直帰線消去期間を利用する以外に、音声副搬送波を利用することもできる。音声副搬送波を用いてデータを放送する場合には、音声信号の空いている 2 チ

ャンネル分の周波数を使ってデータを送る。1 チャンネル当たり約 9.6 kbps の伝送容量があるので、2 チャンネル分では約 19.2 kbps のインターネットデータを放送することができる。

【0108】また、上記の例は、復号化鍵をテレビ映像情報およびテレビ音声情報に対して独立した情報として送信する場合であるが、データハイディング技術（日経エレクトロニクス、No. 683, pp149-162, 1997. 2. 24）を用いて、復号化鍵をテレビ映像情報またはテレビ音声情報に埋め込んで放送してもよい。この場合には、復号化鍵抽出部 8 を、アナログ復調部 2 からの映像情報または音声情報から復号化鍵を抽出して、システムバス 4 に出力するものとする。

【0109】このように、テレビ映像情報またはテレビ音声情報に復号化鍵を埋め込んで放送する場合には、ビデオ録画した後でも、録画されたテレビ映像情報またはテレビ音声情報の中に復号化鍵を保持できるので、ビデオ映像を再生表示しながら、ビデオ映像に関連した秘匿情報を復号化して表示できるようになる。

【0110】また、上記の例は、放送局が秘匿データを放送する場合であるが、秘匿データを視聴者に配信する方法としては、放送局などが秘匿データを CDROM などの記憶媒体に記憶させて、この記憶媒体そのものを視聴者に配布するようにしてもよい。この場合には、その記録媒体が秘匿情報記憶部 6 を構成することになる。

【0111】さらに、上述した第 1 の実施形態は、デジタルテレビ放送の送受信システムにも適用することができる。例えば、人工衛星を利用した衛星デジタルテレビ放送でも、デジタル化したテレビ映像情報およびテレビ音声情報に HTML 書式のインターネットデータを多重化して放送する試みが開始されており、この衛星データ放送を受信する場合には、約 1.5 Mbps で高速伝送されるインターネットデータを受信することができる。

【0112】（効果）上述した第 1 の実施形態によれば、テレビ番組を視聴した人だけが知ることができる秘匿情報をテレビ番組の放送に先立って予め配信することができ、秘匿情報を不特定多数の視聴者に対して配信する場合でも、テレビ番組を見た視聴者だけに情報を知る権利を与えることができる。

【0113】また、テレビ番組の進行に合わせて、情報の公開・非公開を動的に変更することができるとともに、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができる。

【0114】さらに、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビ番組に集中できるようになる。また、CDROM などの放送以外のメディアによって視聴者に提供された秘匿情報でも、テレビ番組に連動させて復号化して再生することができる。

【0115】〔第 2 の実施形態〕第 1 の実施形態は、放

送局が、不特定多数の視聴者に対して、暗号化されたWebページを予め配信しておき、テレビ番組を見た視聴者だけが、その秘匿Webページの内容を見ることができるようにした場合である。

【0116】これに対して、第2の実施形態は、情報提供者が許可した特定の視聴者だけにアクセスを許すWebページを放送する場合である。すなわち、第2の実施形態では、放送局は、秘匿Webページをテレビ番組の開始に先立って放送し、放送局（情報提供者）が許可した視聴者だけが、テレビ番組の進行に合わせて、その秘匿Webページを読み出して見ることができるようにする。

【0117】また、第2の実施形態は、この発明を衛星デジタルテレビ放送の送受信システムに適用した場合である。この衛星デジタルテレビ放送を受信する受信機は、例えば、日本国内で放送が開始されているPerfecTV!放送を受信する受信機である。

【0118】（構成）第2の実施形態では、テレビ受信機にはICカードを装着できるようにする。図10に示すように、このICカード81内には、メモリ部82のほかには演算部83を設け、メモリ部82には、ユーザID、およびユーザ鍵Kuを記憶させる。演算部83は、後述するように鍵復号化演算を行うものである。

【0119】ユーザ鍵Kuは、視聴者が放送によって配信された秘匿データを復号化する権利を有するか否かを識別するために用いられる鍵であって、各視聴者ごとに異なるものである。なお、衛星デジタルテレビ放送などの、映像スクランブルの復号に用いられている、視聴者ごとに異なる復号化鍵を、この実施形態のユーザ鍵Kuとして用いてもよい。

【0120】第2の実施形態では、放送局は、図9に示すように、放送局データベース71として、放送データを管理するための放送データ管理データベース72と、ユーザ情報を管理するためのユーザ管理データベース73とを備え、放送データ管理データベース72には、放送データ、暗号化／復号化鍵Ke、および秘匿データ特定情報を保持し、ユーザ管理データベース73には、宛先ユーザID、および宛先ユーザのユーザ鍵Kuを保持するものとする。

【0121】放送データ管理データベース72の放送データは、暗号化して秘匿データとするデータである。

【0122】鍵Keは、その放送データを暗号化するための暗号化鍵であり、かつ、この鍵Keによって暗号化された秘匿データを復号化するための復号化鍵である。すなわち、第2の実施形態では、情報を暗号化するための暗号化鍵と、この暗号を解くための復号化鍵とが同一の鍵である共有鍵暗号方式を用いる。

【0123】ただし、データを暗号化する暗号化方式としては、共有鍵暗号方式以外にも、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせた

ハイブリッド暗号方式を用いてもよい。例えば、公開鍵暗号方式を用いる場合には、暗号化鍵Keと復号化鍵Keとは、公開鍵ペアとなるように生成する。

【0124】放送データ管理データベース72の秘匿データ特定情報は、秘匿データを特定するための識別情報であり、例えば、放送番組識別子としてのGコード、およびデジタルデータ識別子である。

【0125】ユーザ管理データベース73のユーザ鍵Kuは、上記の鍵Keを暗号化する鍵である。すなわち、放送局のユーザ管理データベース73には、各視聴者が保持するICカード81に記憶されているユーザ鍵（第2の復号化鍵）Kuと同一のユーザ鍵（第2の暗号化鍵）Kuが保持される。したがって、ユーザ管理データベース73に保持されるユーザ鍵Kuで暗号化された復号化鍵Keは、視聴者が保持するICカード81に記憶されているユーザ鍵Kuで復号化することによって、取り出せることになる。

【0126】なお、この場合も、公開鍵暗号方式、または公開鍵暗号方式と共有鍵暗号方式とを組み合わせたハイブリッド暗号方式を用いてもよい。例えば、ユーザ管理データベース73に保持されるユーザ鍵Kuと、各視聴者が保持するICカード81に記憶されているユーザ鍵Kuとを、公開鍵ペアとなるように生成する。

【0127】（秘匿データ受信記憶時の動作）テレビ番組の開始に先立って、放送局は秘匿データを放送し、テレビ受信機は、その放送された秘匿データを受信して秘匿情報記憶部に記憶する。

【0128】具体的に、図11に示すように、テレビ放送局70では、暗号化すべき放送データごとにランダムな暗号化鍵Keを作成して、データ暗号化部74において、その暗号化鍵Keで放送データを暗号化し、その暗号化された秘匿データを、テレビ番組の開始時刻より前の時点において放送する。

【0129】この場合、MIMEエンコーダ75において、その暗号化された秘匿データに対して、この秘匿データを受信すべき視聴者を指定する宛先ユーザIDリストと、この秘匿データを後から特定できるようにするための秘匿データ特定情報、例えば上記のGコードおよびデジタルデータ識別子とを、多重化して放送する。

【0130】図12に示すように、テレビ受信機40では、MIMEデコーダ21によって、テレビ放送局70からの多重化された放送信号から、暗号化された秘匿データ、宛先ユーザIDリスト、および秘匿データ特定情報を分離し、宛先照合部22において、宛先ユーザIDリスト中に、ICカード81に記憶されている自分のユーザIDが含まれているか否かを照合する。

【0131】そして、宛先ユーザIDリスト中に自分のユーザIDが含まれている場合には、受信した秘匿データおよび秘匿データ特定情報を自分宛てのものとして、その秘匿データおよび秘匿データ特定情報を秘匿情報記

10

20

30

40

50

憶部 6 に記憶する。この場合、秘匿情報記憶部 6 は、図 5 に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶する。

【0132】（秘匿データ復号再生時の動作）放送局は、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化鍵 K_e を、その秘匿データを正しく復号化する権利を有する視聴者のユーザ鍵 K_u によって暗号化して、テレビ番組の進行に合わせて放送する。

【0133】すなわち、図 13 に示すように、テレビ放送局 70 では、鍵暗号化部 76 において、復号化鍵 K_e （秘匿データを暗号化したときの暗号化鍵 K_e と同一の鍵）を、宛先視聴者に固有のユーザ鍵 K_u （宛先視聴者の IC カード 81 内のユーザ鍵 K_u と同一の鍵）によって、宛先視聴者の数だけ暗号化し、その暗号化された復号化鍵 $K_{e'}$ のリストを、テレビ番組の進行に合わせて放送する。

【0134】この場合、MIME エンコーダ 75 において、その暗号化された復号化鍵 $K_{e'}$ のリストに対して、この復号化鍵 $K_{e'}$ の宛先視聴者を指定する宛先ユーザ ID リストと、この復号化鍵 $K_{e'}$ によって復号化されるべき秘匿データを特定するための秘匿データ特定情報、例えば上記の G コードおよびデジタルデータ識別子とを、多重化して放送する。

【0135】図 14 に示すように、テレビ受信機 40 では、MIME デコーダ 21 によって、テレビ放送局 70 からの多重化された放送信号から、暗号化された復号化鍵 $K_{e'}$ のリスト、宛先ユーザ ID リスト、および秘匿データ特定情報を分離し、宛先照合部 22 において、宛先ユーザ ID リスト中に、IC カード 81 のメモリ部 82 に記憶されている自分のユーザ ID が含まれているかを照合する。

【0136】そして、宛先ユーザ ID リスト中に自分のユーザ ID が含まれている場合には、受信した暗号化された復号化鍵 $K_{e'}$ および秘匿データ特定情報を自分宛てのものとして、IC カード 81 内の演算部 83 において、その暗号化された復号化鍵 $K_{e'}$ を、自分が IC カード 81 のメモリ部 82 内に所有する、自分に固有のユーザ鍵 K_u によって復号化して、復号化鍵 K_e を取り出す。

【0137】同時に、宛先ユーザ ID リスト中に自分のユーザ ID が含まれている場合には、秘匿情報特定部 7 は、秘匿情報記憶部 6 に記憶されている秘匿データのうちの、MIME デコーダ 21 により分離された秘匿データ特定情報によって特定される秘匿データを特定し、さらに秘匿情報復号化部 9 は、その秘匿情報特定部 7 によって特定されて秘匿情報記憶部 6 から読み出された秘匿データを、IC カード 81 内の演算部 83 から得られた復号化鍵 K_e によって復号化する。

【0138】その復号化された秘匿データは、秘匿情報再生部 10 によって処理されて、映像・音声・データ出力部 3 に出力され、テレビ受信機 40 の表示画面に表示される。

【0139】（効果）この第 2 の実施形態によれば、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機 40 を改造した場合でも、テレビ放送局 70 が復号化鍵 K_e の暗号化の際に用いたユーザ鍵 K_u と、視聴者の IC カード 81 に記憶されているユーザ鍵 K_u とが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【0140】〔第 3 の実施形態〕第 2 の実施形態は、情報提供者が許可した特定の視聴者だけにアクセスを許す Web ページを放送する場合に、すでに放送した秘匿 Web ページを復号化するための復号化鍵 K_e を、宛先視聴者に固有のユーザ鍵 K_u によって、宛先視聴者の数だけ暗号化して、放送するもので、放送局の放送システムおよび受信側の受信システムを比較的簡単にできる特長があるが、テレビ番組と同期したタイミングで、宛先視聴者ごとに異なる暗号化された復号化鍵 $K_{e'}$ を放送するため、宛先視聴者の数が多い場合には、テレビ番組の進行に合わせて復号化鍵を送信することが困難になる可能性がある。

【0141】そこで、第 3 の実施形態は、テレビ番組の開始に先立って秘匿データを放送する際に、当該秘匿データを復号化するための復号化鍵を暗号化して、秘匿データとともに放送し、その後、テレビ番組の進行に合わせて、先に放送した暗号化された復号化鍵を復号化するための復号化鍵を放送し、これによって得られた復号化鍵を用いて当該秘匿データを復号化するものである。

【0142】この場合、秘匿データとともに放送する暗号化された復号化鍵は、各視聴者ごとに異なる個別復号化鍵とし、テレビ番組の進行に合わせて放送する復号化鍵は、全視聴者に共通の共通復号化鍵とする。

【0143】この第 3 の実施形態によれば、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに 1 つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【0144】第 3 の実施形態も、第 2 の実施形態と同様に、この発明を衛星デジタルテレビ放送の送受信システムに適用した場合である。この衛星デジタルテレビ放送を受信する受信機は、例えば、日本国内で放送が開始されている Perfect V! 放送を受信する受信機である。

【0145】（構成）第 3 の実施形態でも、第 2 の実施形態と同様に、テレビ受信機には IC カードを装着できるようにする。第 2 の実施形態と同様に、図 10 に示す

10

20

30

40

50

ように、この IC カード 81 のメモリ部 82 には、ユーザ鍵 Ku を記憶させる。第 2 の実施形態と同様に、このユーザ鍵 Ku は、視聴者が放送によって配信された秘匿データを復号化する権利を有するか否かを識別するために用いられる鍵であって、各視聴者ごとに異なるものである。

【0146】第 2 の実施形態と同様に、IC カード 81 は内部に演算部 83 を備えるものとする。また、第 3 の実施形態では、図 17 に示すように、テレビ受信機 40 は、さらに暗号化鍵記憶部 23 を備えるものとする。

【0147】放送局データベース 71 については、第 3 の実施形態では、図 15 に示すように、放送データ管理データベース 72 には、上述した第 1 の暗号化鍵としての暗号化／復号化鍵 Ke とともに、第 3 の暗号化鍵としての暗号化／復号化鍵 Kc を保持するようにする。ユーザ管理データベース 73 には、第 2 の暗号化鍵としてのユーザ鍵 Ku を保持することは、第 2 の実施形態と同じである。

【0148】第 3 の暗号化鍵としての暗号化／復号化鍵 Kc は、テレビ番組の進行に合わせて放送する鍵であって、全視聴者に共通のものである。

【0149】(秘匿データ受信記憶時の動作) テレビ番組の開始に先立って、放送局は、上記の第 1 暗号化鍵 Ke を第 2 暗号化鍵 Ku で暗号化し、その暗号化された暗号化鍵 Ke' を、さらに第 3 暗号化鍵 Kc で暗号化して、その暗号化された暗号化鍵 Ke'' と、秘匿データとを放送し、テレビ受信機は、その放送された秘匿データおよび暗号化された暗号化鍵 Ke'' を受信して、秘匿データを秘匿情報記憶部に記憶し、暗号化された暗号化鍵 Ke'' を上記の暗号化鍵記憶部に記憶する。

【0150】すなわち、図 16 に示すように、テレビ放送局 70 では、暗号化すべき放送データごとにランダムな第 1 暗号化鍵 Ke および第 3 暗号化鍵 Kc を作成して、データ暗号化部 74 において、その第 1 暗号化鍵 Ke で放送データを暗号化し、その暗号化された秘匿データを、MIME エンコーダ 75 に送出する。

【0151】また、鍵暗号化部 76 において、第 1 復号化鍵 Ke を、宛先視聴者に固有の第 2 暗号化鍵 (ユーザ鍵) Ku によって、宛先視聴者の数だけ暗号化して、その暗号化された暗号化鍵 Ke' のリストを得る。さらに、鍵暗号化部 77 において、その暗号化された暗号化鍵 Ke' のリストを、第 3 暗号化鍵 Kc で暗号化して、その暗号化された暗号化鍵 Ke'' のリストを、MIME エンコーダ 75 に送出する。

【0152】そして、MIME エンコーダ 75 において、暗号化された秘匿データ、暗号化された暗号化鍵 Ke'' のリスト、宛先ユーザ ID リスト、および秘匿データ特定情報を多重化して、テレビ番組の開始時刻より前の時点において放送する。

【0153】図 17 に示すように、テレビ受信機 40 で

は、MIME デコーダ 21 によって、テレビ放送局 70 からの多重化された放送信号から、暗号化された秘匿データ、暗号化された暗号化鍵 Ke'' のリスト、宛先ユーザ ID リスト、および秘匿データ特定情報を分離し、宛先照合部 22 において、宛先ユーザ ID リスト中に、IC カード 81 に記憶されている自分のユーザ ID が含まれているか否かを照合する。

【0154】そして、宛先ユーザ ID リスト中に自分のユーザ ID が含まれている場合には、受信した秘匿データおよび暗号化された暗号化鍵 Ke'' などを自分宛のものとして、その秘匿データおよび秘匿データ特定情報を秘匿情報記憶部 6 に記憶するとともに、暗号化された暗号化鍵 Ke'' を暗号化鍵記憶部 23 に記憶する。

【0155】この場合、秘匿情報記憶部 6 は、図 5 に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶するとともに、記憶された秘匿データの秘匿情報記憶部 6 における記憶位置 (図 5 の No カラムの値) を、暗号化鍵記憶部 23 に出力し、暗号化鍵記憶部 23 は、図 18 に示すように、暗号化された暗号化鍵 Ke'' と、秘匿情報記憶部 6 から入力された、秘匿データの秘匿情報記憶部 6 における記憶位置とを、対応づけて記憶する。

【0156】(秘匿データ復号再生時の動作) 放送局は、上記の第 3 暗号化鍵 Kc を、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化鍵として、テレビ番組の進行に合わせて放送する。

【0157】すなわち、図 19 に示すように、テレビ放送局 70 では、MIME エンコーダ 75 において、復号化鍵 (第 3 暗号化鍵) Kc と、この復号化鍵 Kc によって復号化されるべき秘匿データを特定するための秘匿データ特定情報とを、多重化して、テレビ番組の進行に合わせて放送する。

【0158】図 20 に示すように、テレビ受信機 40 では、MIME デコーダ 21 によって、テレビ放送局 70 からの多重化された放送信号から、復号化鍵 Kc、および秘匿データ特定情報を分離する。そして、秘匿情報特定部 7 は、秘匿情報記憶部 6 に記憶されている秘匿データのうちの、MIME デコーダ 21 により分離された秘匿データ特定情報によって特定される秘匿データを特定して、その特定した秘匿データの秘匿情報記憶部 6 における記憶位置を、秘匿情報記憶部 6 から暗号化鍵記憶部 23 に出力させる。

【0159】これによって、図 18 に示したように秘匿データの秘匿情報記憶部 6 における記憶位置に対応して暗号化鍵記憶部 23 に記憶されている、暗号化された暗号化鍵 Ke'' が、暗号化鍵記憶部 23 から鍵復号化部 24 に出力され、鍵復号化部 24 において、暗号化された暗号化鍵 Ke'' が、MIME デコーダ 21 により分離された復号化鍵 Kc によって復号化されて、鍵復号化部 24 から、暗号化された暗号化鍵 Ke' が出力される。

【0160】さらに、ICカード81内の演算部83において、その暗号化された暗号化鍵K_{e'}が、ICカード81のメモリ部82に記憶されているユーザ鍵K_uによって復号化されて、演算部83から、復号化鍵（第1暗号化鍵）K_eが得られる。

【0161】そして、秘匿情報復号化部9において、秘匿情報特定部7によって特定されて秘匿情報記憶部6から読み出された秘匿データが、演算部83から得られた復号化鍵K_eによって復号化される。その復号化された秘匿データは、秘匿情報再生部10によって処理されて、映像・音声・データ出力部3に出力され、テレビ受信機40の表示画面に表示される。

【0162】（効果）この第3の実施形態によれば、第2の実施形態と同様に、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機40を改造した場合でも、テレビ放送局70が復号化鍵K_eの暗号化の際に用いたユーザ鍵K_uと、視聴者のICカード81に記憶されているユーザ鍵K_uとが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【0163】さらに、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに1つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【0164】〔第4の実施形態〕第4の実施形態は、第3の実施形態の変形である。図16に示したように、第3の実施形態では、放送局は、放送データを暗号化した第1暗号化鍵K_eを、宛先視聴者に固有の第2暗号化鍵（ユーザ鍵）K_uで、宛先視聴者の数だけ暗号化し、その後、さらに全視聴者に共通の第3暗号化鍵K_cで暗号化する場合である。

【0165】これに対して、第4の実施形態では、放送局は、放送データを暗号化した第1暗号化鍵K_eを、全視聴者に共通の第3暗号化鍵K_cで暗号化した後に、宛先視聴者に固有の第2暗号化鍵（ユーザ鍵）K_uで、宛先視聴者の数だけ暗号化する。

【0166】これによって、放送局の暗号化処理時間を短縮することができる。さらに、この第4の実施形態によれば、テレビ受信機がテレビ番組の進行に合わせてデータを復号化する際に、ICカードにアクセスする必要がなくなるという効果がある。

【0167】（秘匿データ受信記憶時の動作）テレビ番組の開始に先立って、放送局は、上記の第1暗号化鍵K_eを第3暗号化鍵K_cで暗号化し、その暗号化された暗号化鍵K_{e'}を、さらに第2暗号化鍵K_uで暗号化して、その暗号化された暗号化鍵K_{e''}と、秘匿データとを放送する。

【0168】すなわち、図21に示すように、テレビ放送局70では、暗号化すべき放送データごとにランダム

な第1暗号化鍵K_eおよび第3暗号化鍵K_cを作成して、データ暗号化部74において、その第1暗号化鍵K_eで放送データを暗号化し、その暗号化された秘匿データを、MIMEエンコーダ75に送出する。

【0169】また、鍵暗号化部76において、第1復号化鍵K_eを、全視聴者に共通の第3暗号化鍵K_cによって暗号化して、その暗号化された暗号化鍵K_{e'}を得る。さらに、鍵暗号化部77において、その暗号化された暗号化鍵K_{e'}を、宛先視聴者に固有の第2暗号化鍵（ユーザ鍵）K_uによって、宛先視聴者の数だけ暗号化して、その暗号化された暗号化鍵K_{e''}のリストを、MIMEエンコーダ75に送出する。

【0170】そして、MIMEエンコーダ75において、暗号化された秘匿データ、暗号化された暗号化鍵K_{e''}のリスト、宛先ユーザIDリスト、および秘匿データ特定情報を多重化して、テレビ番組の開始時刻より前の時点において放送する。

【0171】図22に示すように、テレビ受信機40では、MIMEデコーダ21によって、テレビ放送局70からの多重化された放送信号から、暗号化された秘匿データ、暗号化された暗号化鍵K_{e''}のリスト、宛先ユーザIDリスト、および秘匿データ特定情報を分離し、宛先照合部22において、宛先ユーザIDリスト中に、ICカード81に記憶されている自分のユーザIDが含まれているか否かを照合する。

【0172】そして、宛先ユーザIDリスト中に自分のユーザIDが含まれている場合には、受信した秘匿データおよび暗号化された暗号化鍵K_{e''}などを自分宛てのものとして、ICカード81内の演算部83において、その暗号化された暗号化鍵K_{e''}を、自分がICカード81のメモリ部82内に所有する、自分に固有のユーザ鍵K_uによって復号化して、暗号化された暗号化鍵K_{e'}を取り出す。

【0173】そして、MIMEデコーダ21により分離された秘匿データおよび秘匿データ特定情報を秘匿情報記憶部6に記憶するとともに、演算部83から得られた、暗号化された暗号化鍵K_{e'}を暗号化鍵記憶部23に記憶する。

【0174】この場合、秘匿情報記憶部6は、図5に示したように、秘匿データ、その秘匿データについての暗号化方式、および秘匿データ特定情報を、対応づけて記憶するとともに、記憶された秘匿データの秘匿情報記憶部6における記憶位置（図5のNoカラムの値）を、暗号化鍵記憶部23に出力し、暗号化鍵記憶部23は、図23に示すように、暗号化された暗号化鍵K_{e'}と、秘匿情報記憶部6から入力された、秘匿データの秘匿情報記憶部6における記憶位置とを、対応づけて記憶する。

【0175】（秘匿データ復号再生時の動作）放送局は、上記の第3暗号化鍵K_cを、テレビ番組と連動して復号化されるべき秘匿データを復号化するための復号化

10

20

30

40

50

鍵として、テレビ番組の進行に合わせて放送する。

【0176】すなわち、図24に示すように、テレビ放送局70では、MIMEエンコーダ75において、復号化鍵（第3暗号化鍵）Kcと、この復号化鍵Kcによって復号化されるべき秘匿データを特定するための秘匿データ特定情報とを、多重化して、テレビ番組の進行に合わせて放送する。

【0177】図25に示すように、テレビ受信機40では、MIMEデコーダ21によって、テレビ放送局70からの多重化された放送信号から、復号化鍵Kc、および秘匿データ特定情報を分離する。そして、秘匿情報特定部7は、秘匿情報記憶部6に記憶されている秘匿データのうちの、MIMEデコーダ21により分離された秘匿データ特定情報によって特定される秘匿データを特定して、その特定した秘匿データの秘匿情報記憶部6における記憶位置を、秘匿情報記憶部6から暗号化鍵記憶部23に出力させる。

【0178】これによって、図23に示したように秘匿データの秘匿情報記憶部6における記憶位置に対応して暗号化鍵記憶部23に記憶されている、暗号化された暗号化鍵Ke'が、暗号化鍵記憶部23から鍵復号化部24に出力され、鍵復号化部24において、暗号化された暗号化鍵Ke'が、MIMEデコーダ21により分離された復号化鍵Kcによって復号化されて、鍵復号化部24から、復号化鍵（第1暗号化鍵）Keが出力される。

【0179】そして、秘匿情報復号化部9において、秘匿情報特定部7によって特定されて秘匿情報記憶部6から読み出された秘匿データが、鍵復号化部24から得られた復号化鍵Keによって復号化される。その復号化された秘匿データは、秘匿情報再生部10によって処理されて、映像・音声・データ出力部3に出力され、テレビ受信機40の表示画面に表示される。

【0180】（効果）この第4の実施形態によれば、第2または第3の実施形態と同様に、視聴者が不正に他人宛ての秘匿データを受信できるようにテレビ受信機40を改造した場合でも、テレビ放送局70が復号化鍵Keの暗号化の際に用いたユーザ鍵Kuと、視聴者のICカード81に記憶されているユーザ鍵Kuとが一致しない場合には、秘匿データを正しく復号化することができないので、システムの安全性が保証される。

【0181】また、第3の実施形態と同様に、秘匿データを復号化するための復号化鍵の宛先が多い場合でも、テレビ番組の進行に合わせて放送する復号化鍵は、わずかに1つで済むので、テレビ番組の進行に合わせて復号化鍵を送信することが困難になるというようなことは全くない。

【0182】さらに、テレビ受信機40がテレビ番組の進行に合わせてデータを復号化する際に、ICカード81にアクセスする必要がなくなる。

【0183】（その他の実施形態）上述した各実施形態

は、この発明をテレビ放送の送受信システムに適用した場合であるが、この発明はラジオ放送の送受信システムにも適用することができる。

【0184】秘匿情報、またはテレビ放送信号またはラジオ放送信号に重畳されるデータとしては、電波またはケーブルによって伝送されたテレビ放送信号の垂直帰線消去期間に多重化された情報、テレビ放送またはラジオ放送の音声副チャンネルによって伝送された情報、テレビ放送またはラジオ放送の音声副搬送波によって伝送された情報、デジタルテレビ放送に複合化された情報、またはテレビ放送またはラジオ放送の映像情報または音声情報に埋め込まれた隠し情報が考えられるが、この発明は、これらのいずれの場合にも適用することができる。

【0185】〔各種の実施形態と効果〕この発明では、以下のような実施形態にすることによって、それぞれ以下のような効果が得られる。

【0186】（1）放送局は、秘匿データを復号化するための復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化するように構成することにより、不特定多数人に対してデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【0187】（2）テレビ受信機によって、放送された復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化し、この復号化されたデータをテレビ映像番組の進行に合わせてテレビ受信機に表示再生するように構成することにより、テレビ番組を見た視聴者が、このデータの内容を見る場合でも、秘匿データを復号化する操作を強いられず、視聴しているテレビ番組に集中することができる。

【0188】（3）放送局によって放送された復号化鍵を記憶できるように構成することにより、視聴者は、復号化鍵が記憶された後のタイミングにおいて、秘匿データを随時復号化して表示再生することができる。

【0189】（4）放送局が、秘匿データを復号化するための復号化鍵とともに、放送番組識別情報をデータ放送した場合に、テレビ受信機によって、この放送された放送番組識別情報を受信し、記憶媒体に記憶された秘匿データのうちの、放送番組識別情報によって特定されたテレビ番組に関連する秘匿データを復号化鍵によって復号化するように構成することにより、不特定多数の視聴

者に対してテレビ番組に関連するデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【0190】(5) テレビ受信機によって、放送局から放送された復号化鍵を受信した場合に、記憶媒体に記憶された秘匿データのうちの、視聴中のテレビチャンネル番号と復号化鍵受信時刻とに基づいて、記憶媒体に記憶された秘匿データのうちの、受信した復号化鍵に対応する秘匿データを特定するように構成することにより、放送局から放送番組識別情報が放送されなかった場合でも、放送中のテレビ番組に関連する秘匿データを特定することができるので、テレビ番組を見た視聴者だけが秘匿データの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【0191】(6) 秘匿データを、放送局から放送される秘匿データ特定情報によって特定できるように、インデックス情報を付加するなどして、記憶媒体に記憶するように構成することにより、放送中の放映内容に関連する秘匿データを特定することができるので、例えば、同一テレビ番組中であっても、テレビ放送番組の進行に合わせて情報の公開・非公開を動的に変更することができる。

【0192】(7) 放送局が、テレビ番組放送開始時刻より前の時点において秘匿データを放送した場合に、テレビ受信機が、放送された秘匿データを記憶媒体に記憶するように構成することにより、放送局がテレビ番組放送と連動して秘匿データを復号化する復号化鍵を放送した時に、記憶媒体に記憶された秘匿データを復号化鍵によって復号化できるので、テレビ番組放送開始時刻より前の時点において不特定多数の視聴者に対してデータを予め配信しておいた場合でも、テレビ番組を見た視聴者だけが、このデータの内容を見ることができるようになり、これによって、放送局は、テレビ番組を見た視聴者だけに有益なデータを提供することができる。

【0193】(8) 放送局は、秘匿データを復号化するための第1の復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された第1の復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、第1の復号化鍵と、ICカードメモリなどから入力した第2の復号化鍵とによって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することが

できる。

【0194】(9) テレビ受信機によって、放送された第1の復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、第1の復号化鍵と、各視聴者が所有する第2の復号化鍵によって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、秘匿データを復号化する権利を持った視聴者のみがデータの内容を見ることができ、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【0195】(10) 放送局は、秘匿データを復号化するための復号化鍵を暗号化鍵で暗号化して、この暗号化した復号化鍵を、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された暗号化された復号化鍵を、ICカードメモリなどから入力した第2の復号化鍵によって復号化し、これによって取り出した復号化鍵を用いて、秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【0196】(11) 放送局は、秘匿データを復号化するための復号化鍵を暗号化鍵で暗号化して、この暗号化した復号化鍵を、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された暗号化された復号化鍵を、ICカードメモリなどから入力した第2の復号化鍵によって復号化し、これによって取り出した復号化鍵を用いて、秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、秘匿データを復号化する権利を持った視聴者のみがデータの内容を見ることができ、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【0197】(12) 放送局は、秘匿データを復号化するための全視聴者または全受信機に共通の第1の復号化鍵と、この復号化鍵を適用すべき秘匿データを特定する秘匿データ特定情報とを、テレビ映像番組の進行に合わせて放送し、テレビ受信機は、放送された第1の復号化鍵と秘匿データ特定情報とを受信して、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、前記第1の復号化鍵と、ICカードメモリなどから入力した視聴者または受信機ごとに異なる個別の第2の復号化鍵とによって復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができるようになり、これによって、放送局は、特定の視聴者だけに有益なデータを提供することができる。

【0198】(13) 秘匿情報記憶部に記憶された秘匿データが、第1の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第1暗号化鍵に対応した第1の復号化鍵を、視聴者または受信機ごとに異なる個別の第2の暗号化鍵と、第3の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第3の暗号化鍵に対応する第3の復号化鍵と、ICカードメモリなどから入力した第2の暗号化鍵に対応する第2の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第1の復号化鍵を抽出し、この第1の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第3の暗号化鍵に対応する第3の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【0199】(14) 秘匿情報記憶部に記憶された秘匿データが、第1の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報入力部から入力された暗号化鍵情報が、第1の暗号化鍵に対応した第1の復号化鍵を、第3の暗号化鍵を用いて暗号化し、この暗号化した情報をさらに視聴者または受信機ごとに異なる個別の第2の暗号化鍵を用いて暗号化した情報であった場合に、テレビ受信機は、ICカードメモリなどから入力した第2の暗号化鍵に対応する第2の復号化鍵を用いて、暗号化鍵情報入力部から入力された暗号化鍵情報を復号化して、この復号化した暗号化鍵情報を暗号化鍵情報記憶部に記憶するようにし、さらに、テレビ受信機は、テレビ映像番組の進行に合わせて第3の暗号化鍵に対応する第3の復号化鍵が放送された場合に、この第3の復号化鍵によって、暗号化鍵情報記憶部に記憶された暗号化鍵情報を復号化して、第1の暗号化鍵に対応した第1の復号化鍵を抽出し、この第1の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第3の暗号化鍵に対応する第3の復号化鍵を放送するだけでよく、さらに、テレビ受信機は、テレビ番組受信時には、ICカードにアクセスする必要がないために、復号化鍵の宛先視聴者の数が多い場合にも対応でき、かつ、テレビ受信機の秘匿データ復号化処理を高速化することができる。

【0200】(15) 秘匿情報記憶部に記憶された秘匿データが、第1の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第1の暗号化鍵に対応した第2の復号化鍵を、視聴

者または受信機ごとに異なる個別の第2の暗号化鍵と、第3の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第3の暗号化鍵に対応する第3の復号化鍵と、ICカードメモリなどから入力した第2の暗号化鍵と同一の鍵である第2の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第1の復号化鍵を抽出し、この第1の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第3の暗号化鍵に対応する第3の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【0201】(16) 秘匿情報記憶部に記憶された秘匿データが、第1の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第1の暗号化鍵に対応した第1の復号化鍵を、視聴者または受信機ごとに異なる個別の第2の暗号化鍵と、第3の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第3の暗号化鍵に対応する第3の復号化鍵と、ICカードメモリなどから入力した第2の暗号化鍵と公開鍵ペアである第2の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第1の復号化鍵を抽出し、この第1の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第3の暗号化鍵に対応する第3の復号化鍵を放送するだけでよく、さらに、視聴者が保有する第2の復号鍵を放送局に秘密にすることができる。

【0202】(17) 秘匿情報記憶部に記憶された秘匿データが、全視聴者または全受信機に共通の第1の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報記憶部に記憶された暗号化鍵情報が、第1の暗号化鍵に対応した第1の復号化鍵を、視聴者または受信機ごとに異なる個別の第2の暗号化鍵と、全視聴者または全受信機に共通の第3の暗号化鍵とを用いて暗号化した情報であった場合に、テレビ受信機は、テレビ映像番組の進行に合わせて放送された第3の暗号化鍵に対応する第3の復号化鍵と、ICカードメモリなどから入力した第2の暗号化鍵に対応する第2の復号化鍵とを用いて、暗号化鍵情報記憶部に記憶された暗号化鍵情報から第1の復号化鍵を抽出し、この第1の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人だけにデータを見る

権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第 3 の暗号化鍵に対応する第 3 の復号化鍵を放送するだけでよいので、復号化鍵の宛先視聴者の数が多い場合にも対応することができる。

【0203】(18) 秘匿情報記憶部に記憶された秘匿データが、全視聴者または全受信機に共通の第 1 の暗号化鍵によって暗号化されており、かつ、暗号化鍵情報入力部から入力された暗号化鍵情報が、第 1 の暗号化鍵に対応した第 1 の復号化鍵を、全視聴者または全受信機に共通の第 3 の暗号化鍵を用いて暗号化し、この暗号化した情報をさらに視聴者または受信機ごとに異なる個別の第 2 の暗号化鍵を用いて暗号化した情報であった場合に、テレビ受信機は、ICカードメモリなどから入力した第 2 の暗号化鍵に対応する第 2 の復号化鍵を用いて、暗号化鍵情報入力部から入力された暗号化鍵情報を復号化して、この復号化した暗号化鍵情報を暗号化鍵情報記憶部に記憶するようにし、さらに、テレビ受信機は、テレビ映像番組の進行に合わせて第 3 の暗号化鍵に対応する第 3 の復号化鍵が放送された場合に、この第 3 の復号化鍵によって、暗号化鍵情報記憶部に記憶された暗号化鍵情報を復号化して、第 1 の暗号化鍵に対応した第 1 の復号化鍵を抽出し、この第 1 の復号化鍵を用いて秘匿情報記憶部に記憶された秘匿データを復号化するように構成することにより、不特定多数の視聴者に対してデータを予め配信しておいた場合でも、特定の人のだけにデータを見る権利を与えることができ、しかも、放送局は、テレビ番組放送時には、第 3 の暗号化鍵に対応する第 3 の復号化鍵を放送するだけでよく、さらに、テレビ受信機は、テレビ番組受信時には、ICカードメモリにアクセスする必要があるために、復号化鍵の宛先視聴者の数が多い場合にも対応でき、かつ、テレビ受信機の秘匿データ復号化処理を高速化することができる。

【0204】(19) テレビ受信機によって、放送された復号化鍵と秘匿データ特定情報とを受信し、記憶媒体に記憶された秘匿データのうちの、秘匿データ特定情報によって特定された秘匿データを、復号化鍵によって復号化し、この復号化されたデータをテレビ映像番組の進行に合わせてプリンタに出力して印刷できるように構成することにより、視聴者は、秘匿データを復号化する操作を強いられず、視聴しているテレビ番組に集中することができる。

【0205】

【発明の効果】この発明によれば、テレビまたはラジオの番組を視聴した人だけが知ることができる秘匿情報を番組の放送に先立って予め配信することができ、視聴者が秘匿情報を復号化する操作を強いられず、視聴しているテレビまたはラジオの番組に集中することができ、同一の秘匿情報を複数の場面または番組で利用する場合には、一度配信した秘匿情報を再利用することができるとともに、CDROMなどの放送以外のメディアによって

視聴者に提供された秘匿情報でも、テレビまたはラジオの番組に連動させて復号化して再生することができる。

【0206】さらに、テレビまたはラジオの番組の進行に合わせて、情報の公開・非公開、または情報を知ることができる視聴者を動的に変更することができるとともに、テレビまたはラジオの番組に関連した秘匿情報を不特定多数の視聴者に対して配信する場合でも、特定の視聴者だけに情報を知る権利を与えることができるようになる。

10 【図面の簡単な説明】

【図 1】第 1 の実施形態のシステム構成を示す図である。

【図 2】第 1 の実施形態の機能ブロック構成を示す図である。

【図 3】第 1 の実施形態の受信記憶処理ルーチンを示す図である。

【図 4】第 1 の実施形態の秘匿データの一例を示す図である。

20 【図 5】第 1 の実施形態の秘匿情報記憶部の記憶状態の一例を示す図である。

【図 6】第 1 の実施形態の復号再生処理ルーチンを示す図である。

【図 7】第 1 の実施形態の復号化鍵の一例を示す図である。

【図 8】第 1 の実施形態の復号化鍵記憶部の記憶状態の一例を示す図である。

【図 9】第 2 の実施形態の放送局データベースを示す図である。

30 【図 10】第 2 の実施形態のテレビ受信機に装着される ICカードを示す図である。

【図 11】第 2 の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図 12】第 2 の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図 13】第 2 の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

【図 14】第 2 の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

40 【図 15】第 3 の実施形態の放送局データベースを示す図である。

【図 16】第 3 の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図 17】第 3 の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図 18】第 3 の実施形態の暗号化鍵記憶部の記憶状態の一例を示す図である。

【図 19】第 3 の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

50 【図 20】第 3 の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

【図 2 1】第 4 の実施形態の秘匿データ放送時の放送局の機能構成を示す図である。

【図 2 2】第 4 の実施形態の秘匿データ受信時の受信機の機能構成を示す図である。

【図 2 3】第 4 の実施形態の暗号化鍵記憶部の記憶状態の一例を示す図である。

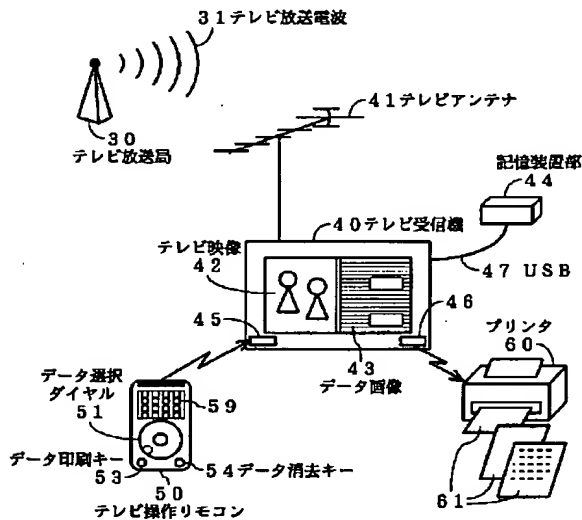
【図 2 4】第 4 の実施形態の復号化鍵放送時の放送局の機能構成を示す図である。

【図 2 5】第 4 の実施形態の復号化鍵受信時の受信機の機能構成を示す図である。

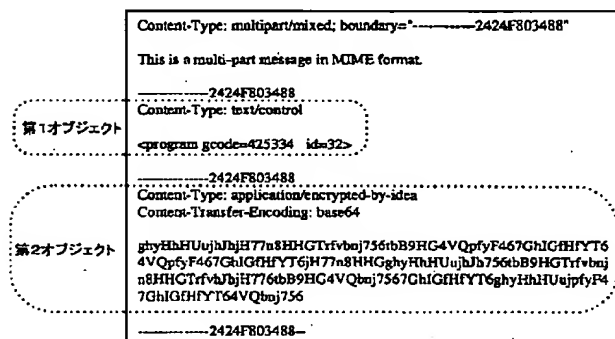
【符号の説明】

- 1 選局部
- 2 アナログ復調部

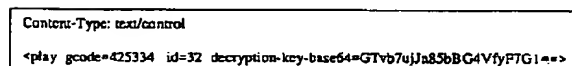
【図 1】



【図 4】

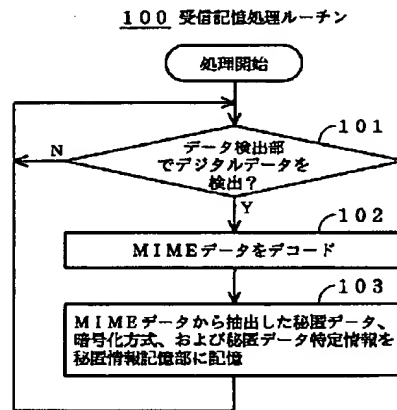


【図 7】



- 3 映像・音声・データ出力部
- 5 データ検出部
- 6 秘匿情報記憶部
- 7 秘匿情報特定部
- 8 復号化鍵抽出部
- 9 秘匿情報復号化部
- 10 秘匿情報再生部
- 11 復号化鍵記憶部
- 30 テレビ放送局
- 40 テレビ受信機
- 50 テレビ操作リモコン
- 60 プリンタ
- 70 テレビ放送局

【図 3】

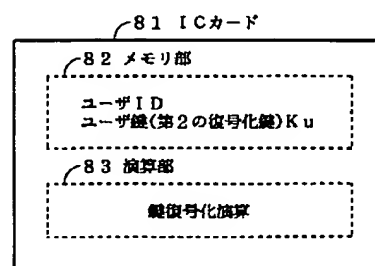


【図 5】

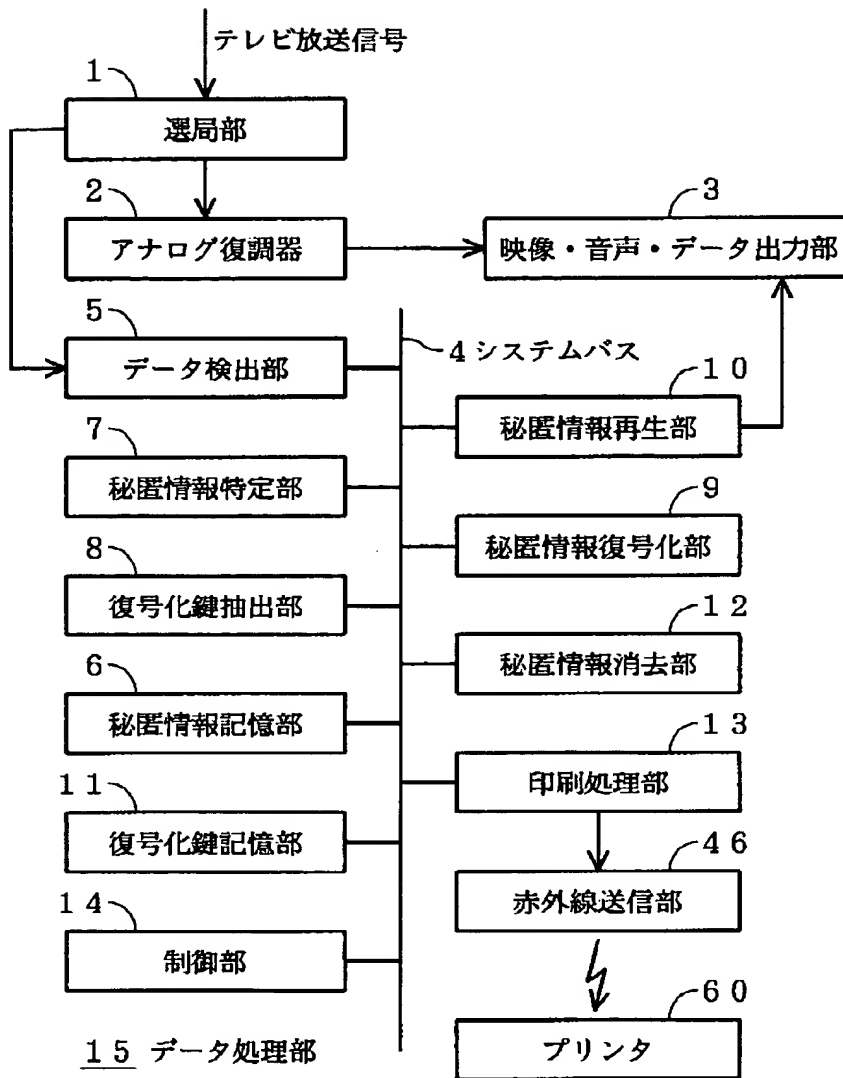
6 秘匿情報記憶部

No.	Gコード	ID	暗号化方式	秘匿データ
10	425334	32	IDEA & Base64	ghyH...bnj756
11	425334	33	IDEA & Base64	thsM...aeR32d
12	86273	1	IDEA & Base64	beD9...Ra3We1
⋮	⋮	⋮	⋮	⋮

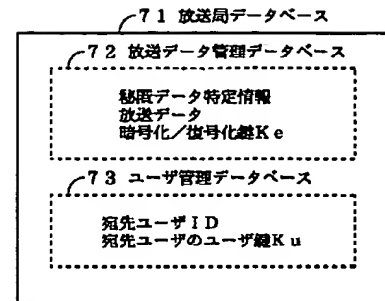
【図 10】



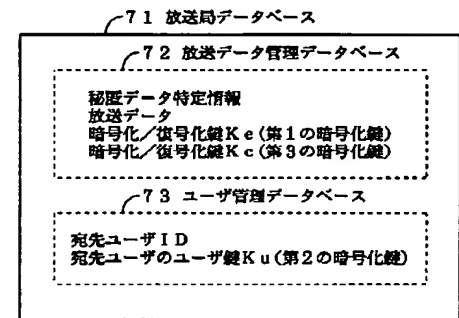
【図 2】



【図 9】



【図 15】

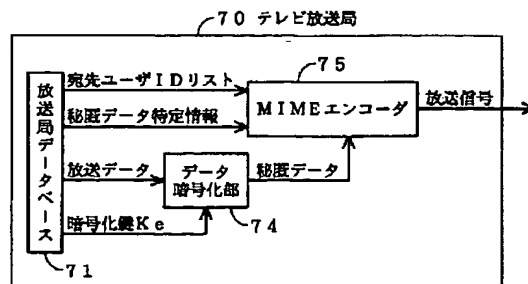


【図 8】

1.1 復号化鍵記憶部

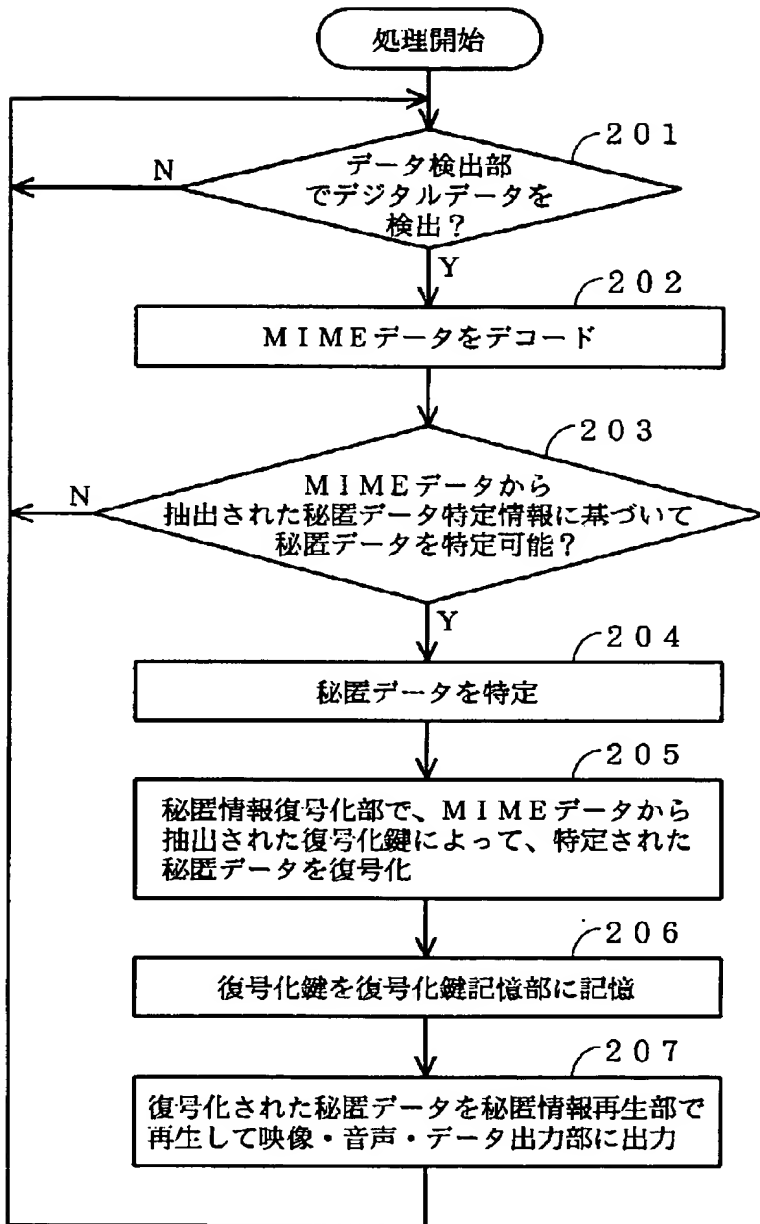
記憶時刻	復号化鍵	秘匿データ記憶位置
1997. 4. 25 19:02 12' 50"	G T v b 7 u j J n 8 5 b B G 4 V f y F 7 G 1 ==	10
1997. 4. 25 19:02 13' 58"	u j J b 2 G r B B F 7 b 8 T v l a f y A 3 ==	11
1997. 4. 25 22:45 48' 06"	7 m 8 G T v z O k G G q 7 F 4 V 3 b B y 4 ==	3
⋮	⋮	⋮
⋮	⋮	⋮

【図 11】

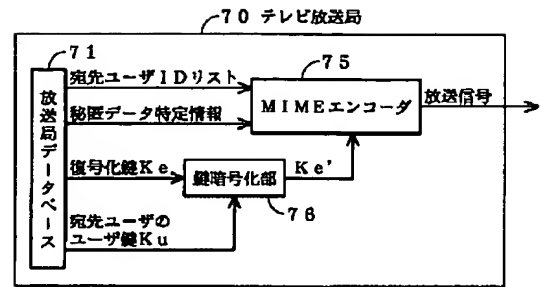


【図6】

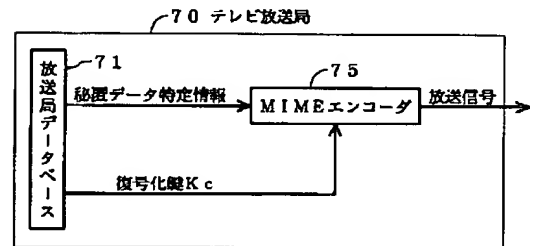
200 復号再生処理ルーチン



【図13】



【図19】

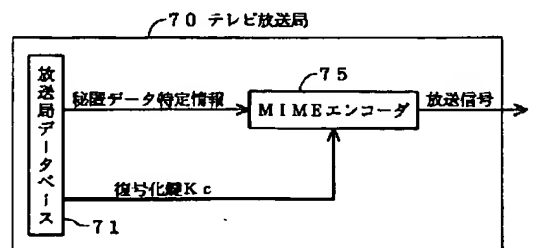


【図23】

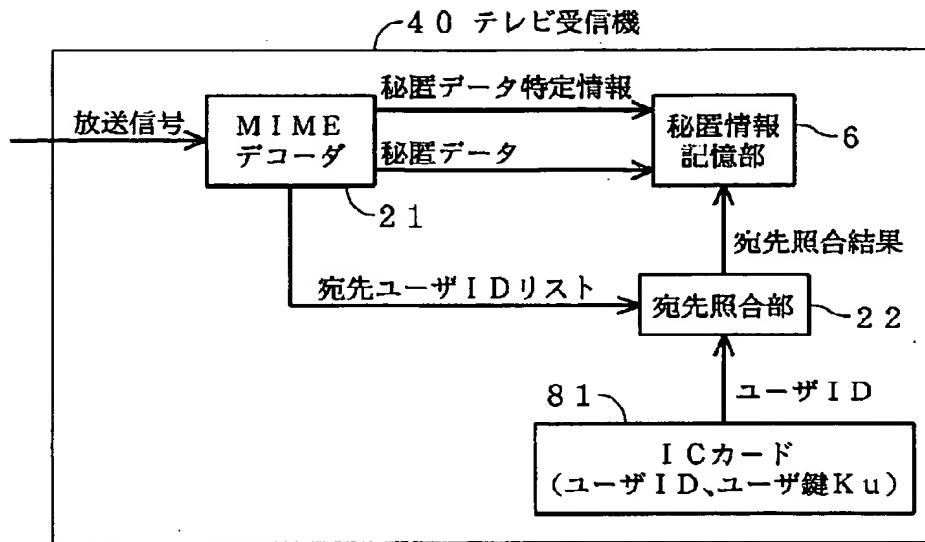
23 暗号化鍵記憶部

No.	暗号化鍵 Ke'	秘匿データ記憶位置
100	78VfyJvGjnA5MFKbB4G1ub==	10
101	v17GfyAur3gBM2F9TjsJbz==	12
102	F4VEyakg3m1b773GGzTvq8==	11
⋮	⋮	⋮

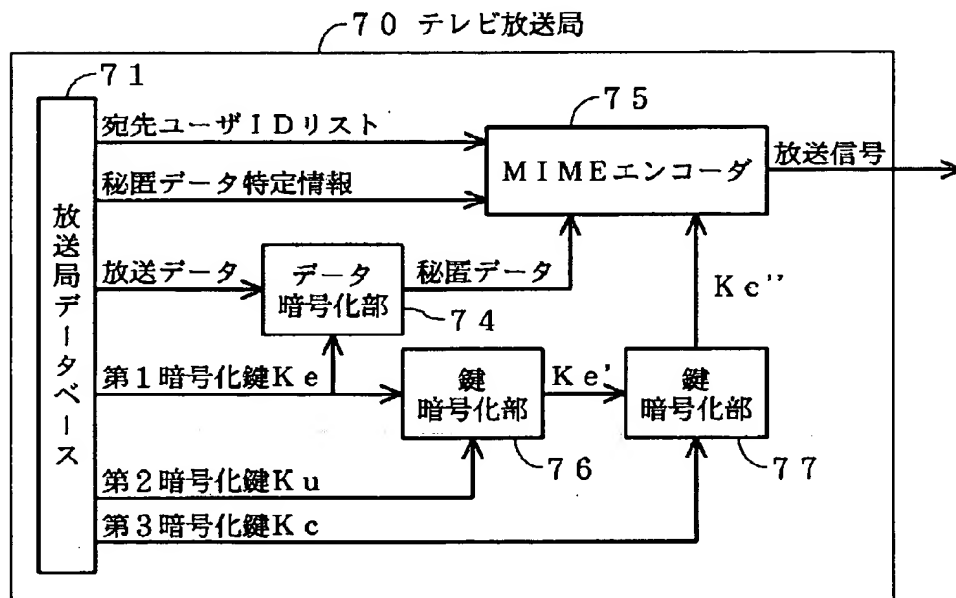
【図24】



【図 12】



【図 16】

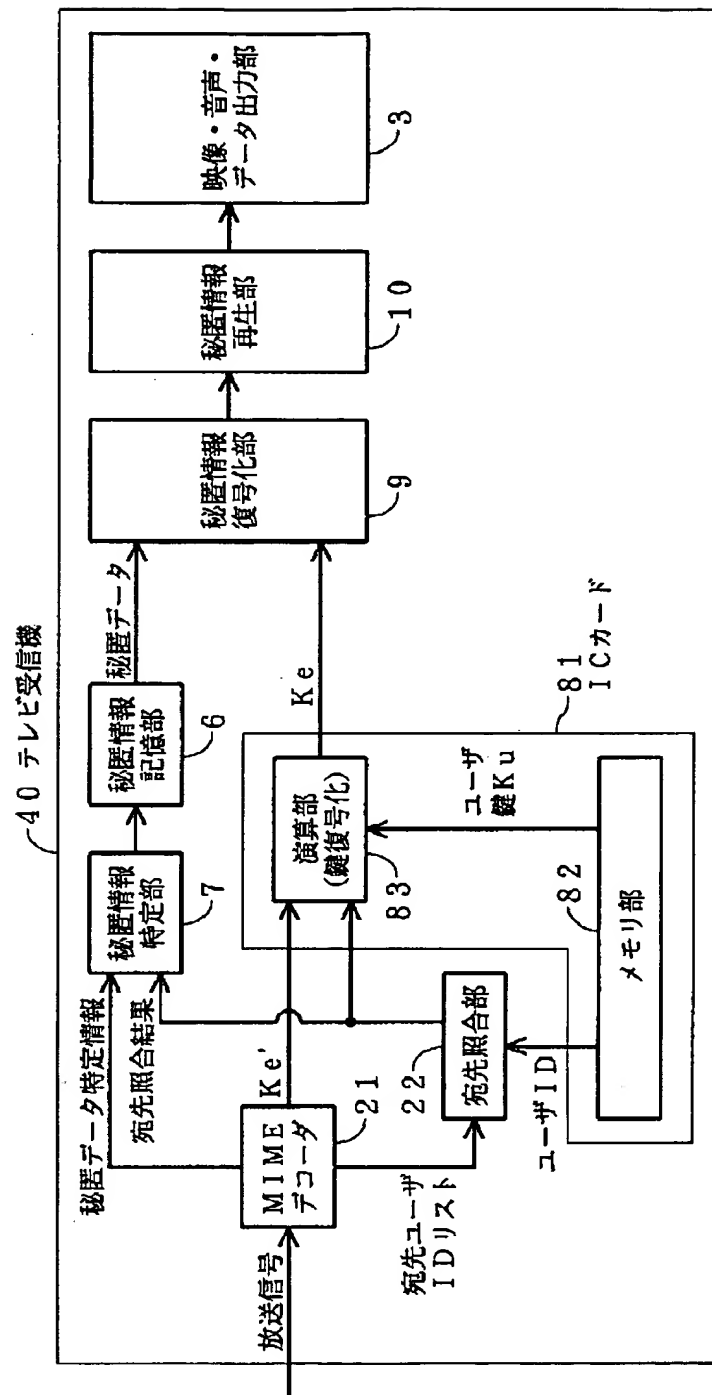


【図 18】

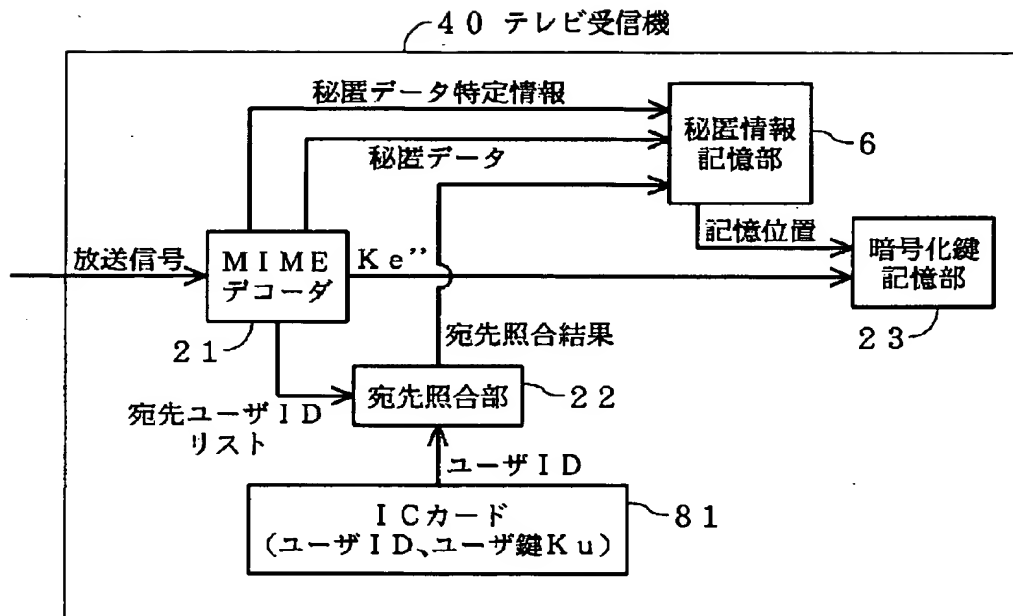
2.3 暗号化鍵記憶部

No.	暗号化鍵Ke''	秘匿データ記憶位置
100	bB4G1ujJvGnGb785TF7Vfy==	10
101	7h2v13GrBBF9ThzfyAujsJ==	12
102	anokG77F4VB3bGzq8GTv4==	11
⋮	⋮	⋮

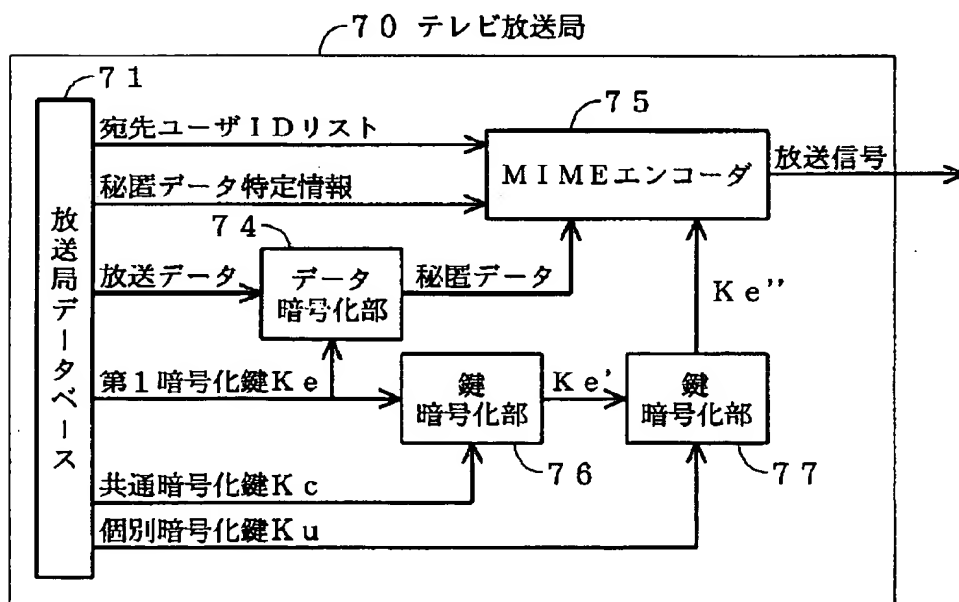
【図 14】



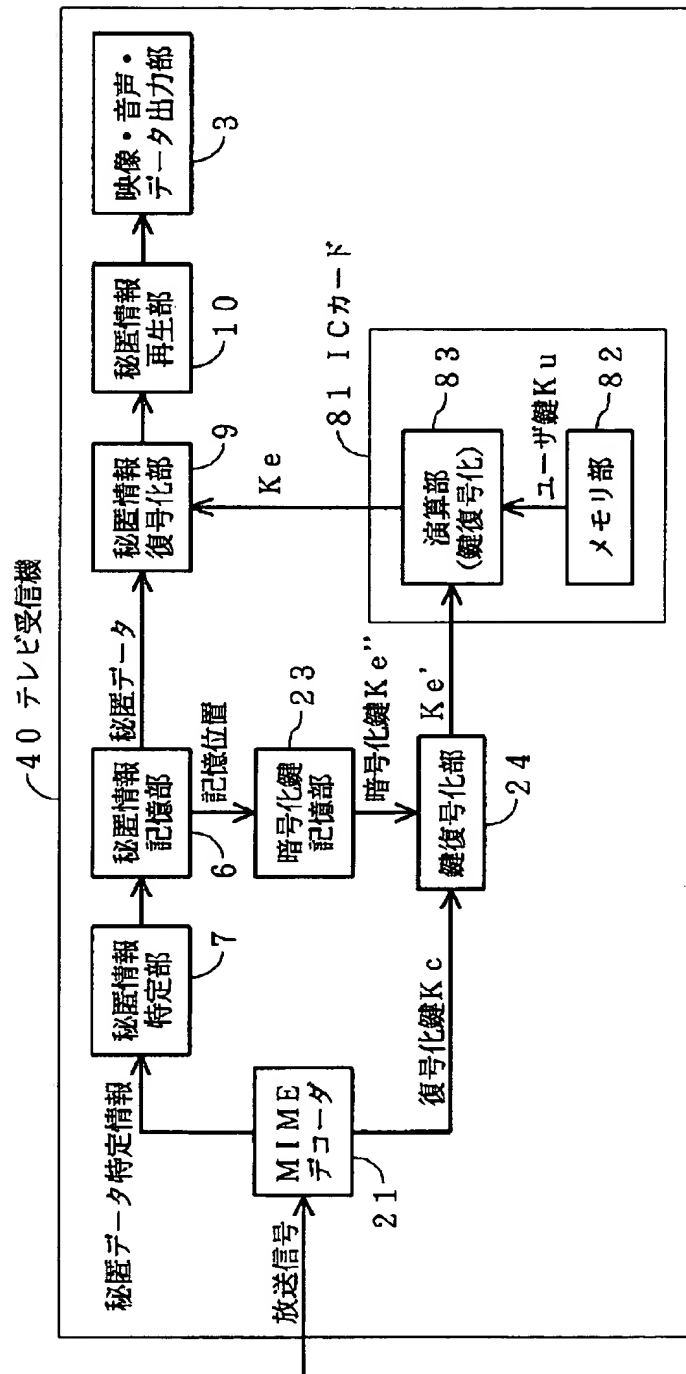
【図17】



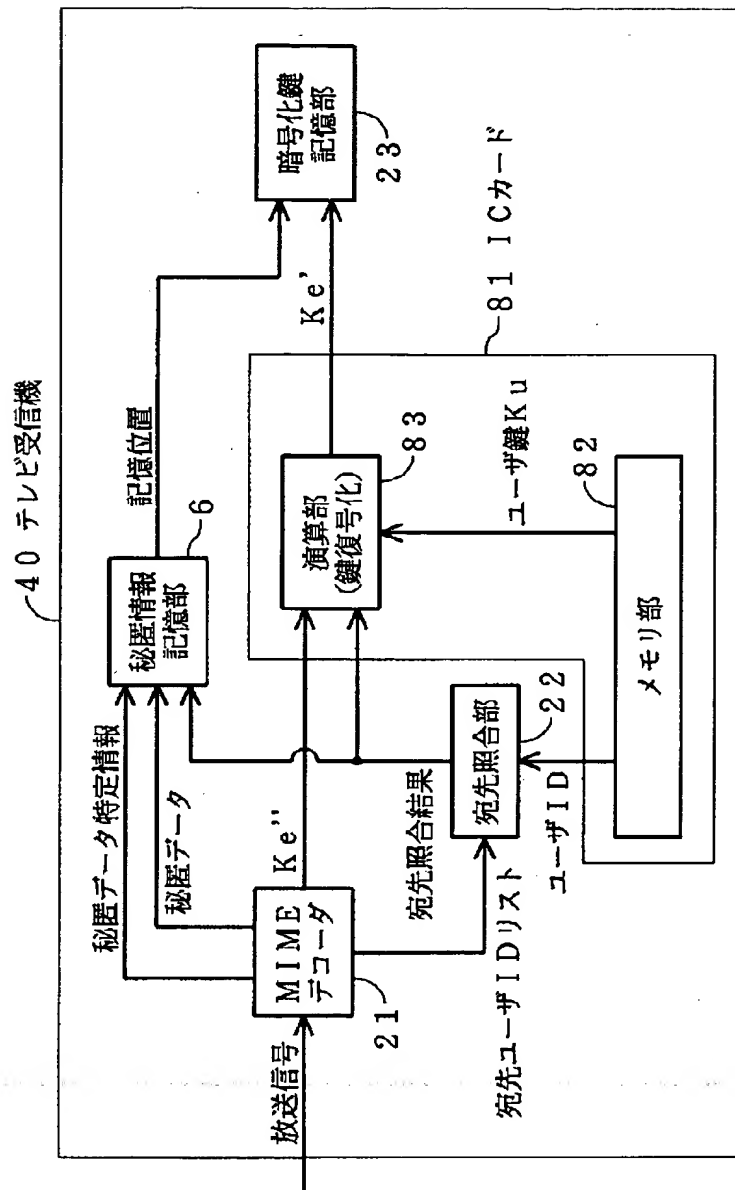
【図21】



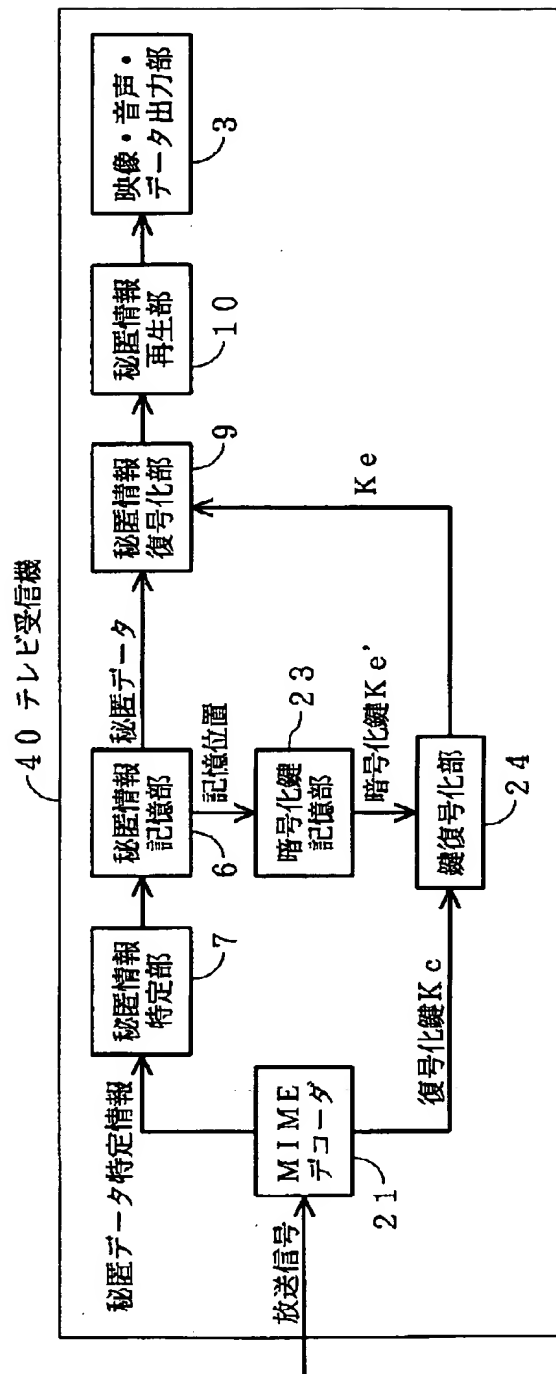
【図 20】



【図22】



【図 2 5】



フロントページの続き

(51) Int. Cl. 6

// H 0 4 N 7/167

識別記号

F I

H 0 4 N 7/167

Z